Docket No. 826.1613/JDH

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Jun IKEGAMI, et al.

Serial No.: Not Assigned

Filed: July 24, 2000

For: AUTHENTICATION DEVICE USING ANATOMICAL INFORMATION AND METHOD THEREOF

Group Art Unit: Not Assigned

Examiner: Not Assigned

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 11-293543, filed: October 15, 1999.

It is respectfully requested that the applicants be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: July 24, 2000

By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 Eleventh Street, N.W., Suite 500
Washington, D.C. 20001
(202) 434-1500

#2

PATENT OFFICE

JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: October 15, 1999

Application Number: Patent Application No. 11-293543

Applicant(s): FUJITSU LIMITED

June 9, 2000

Commissioner,
Patent Office Takahiko Kondo

Certificate No. 2000-3044626

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年１０月１５日

出願番号
Application Number: 平成１１年特許願第２９３５４３号

出願人
Applicant (s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年 ６月 ９日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号 出証特２０００－３０４４６２６

【書類名】　特許願

【整理番号】　9951279

【提出日】　平成11年10月15日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/60

【発明の名称】　生体情報を用いた認証装置及びその方法

【請求項の数】　24

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　池上　潤

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　新崎　卓

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　藤井　勇作

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100074099

【住所又は居所】　東京都千代田区二番町８番地２０　二番町ビル３Ｆ

【弁理士】

【氏名又は名称】　大菅　義之

【電話番号】　03-3238-0031

【選任した代理人】

【識別番号】　100067987

【住所又は居所】　神奈川県横浜市鶴見区北寺尾７－２５－２８－５０３

【弁理士】

【氏名又は名称】　久木元　彰

【電話番号】　045-573-3683

【手数料の表示】

【予納台帳番号】　012542

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705047

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　生体情報を用いた認証装置及びその方法

【特許請求の範囲】

【請求項１】生体情報を用いた認証装置において、

生体情報を取得する生体情報取得手段と、

該生体情報を特定可能な識別情報を生成する識別情報生成手段と、

該識別情報を検証可能な付加情報を生成する付加情報生成手段と、

該生体情報と、該識別情報と該付加情報の少なくとも一方とを暗号化し、暗号化された生体情報と付加情報及び、識別情報を組み合わせて照合情報を生成する照合情報生成手段と、

を備えることを特徴とする装置。

【請求項２】生体情報を用いた認証装置において、

採取した画像から生体情報を生成する生体情報生成手段と、

該生体情報生成手段に内蔵された、生体情報の採取時刻に関するカウンタ値をカウントするカウンタ手段と

該生体情報と該カウンタ手段のカウンタ値とを組み合わせて照合情報を生成する照合情報生成手段と、

を備えることを特徴とする装置。

【請求項３】生体情報を用いた認証装置において、

採取した画像から生体情報を生成する生体情報生成手段と、

該生体情報生成手段を特定する識別情報と、該生体情報生成手段内で生成した生体情報の採取順序を特定する順序情報の少なくともいずれか一方からなる識別情報を生成する識別情報生成手段と

該生体情報と該識別情報とを組み合わせて照合情報を生成する照合情報生成手段と、

を備えることを特徴とする装置。

【請求項４】生体情報を用いた認証装置において、

採取した画像から生体情報を生成する生体情報生成手段と、

外部から提供された情報から識別情報を生成する識別情報生成手段と、

該生体情報と該識別情報とを組み合わせて照合情報を生成する照合情報生成手段と、

を備えることを特徴とする装置。

【請求項５】生体情報を採取する採取装置から認証を行う認証装置をネットワークで接続した、生体情報を用いた認証システムにおいて、

採取した画像から生体情報を生成する生体情報生成手段と、

採取装置から認証装置にいたる経路情報からなる識別情報を生成する識別情報生成手段と、

該生体情報と該識別情報とを組み合わせて照合情報を生成する照合情報生成手段と、

を備えることを特徴とする装置。

【請求項６】生体情報を用いた認証装置であって、

生体情報を予め登録してある登録情報と照合する生体情報照合手段と、

生体情報と共に送信されてくる識別情報が所定の条件を満足するかを判定する識別情報判定手段と、

付加情報に写像演算を行うことによって得られる演算値によって識別情報を検証する識別情報検証手段と、

を備えることを特徴とする装置。

【請求項７】生体情報を用いた認証装置であって、

生体情報を予め登録してある登録情報と照合する生体情報照合手段と、

生体情報と共に送信されてくる識別情報が所定の条件を満足するかを判定する識別情報判定手段と、

を備えることを特徴とする装置。

【請求項８】生体情報を用いた認証装置であって、

生体情報を取得する生体情報取得手段と、

該生体情報の取得された環境を一意に指定可能な識別情報を取得する識別情報取得手段と、

生体情報と識別情報とを暗号化して送信する暗号化・送信手段と、

を備えることを特徴とする装置。

【請求項９】生体情報を用いた認証を行うための照合情報生成方法であって、

生体情報を取得するステップと、

該生体情報を特定可能な識別情報を生成するステップと、

該識別情報を検証可能な付加情報を生成するステップと、

該生体情報と、該識別情報と該付加情報の少なくとも一方とを暗号化し、暗号化された生体情報と付加情報及び、識別情報を組み合わせて照合情報を生成するステップと、

を備えることを特徴とする方法。

【請求項１０】生体情報を用いた認証を行うための照合情報を生成する方法であって、

採取した画像から生体情報を生成するステップと、

該生体情報生成ステップで生体情報が採取された時刻に関するカウンタ値を取得するステップと

該生体情報と該カウンタ値とを組み合わせて照合情報を生成するステップと、

を備えることを特徴とする方法。

【請求項１１】生体情報を用いた認証を行うための照合情報を生成する方法であって、

採取した画像から生体情報を生成するステップと、

該生体情報の生成環境を特定する識別情報を生成するステップと

該生体情報と該識別情報とを組み合わせて照合情報を生成するステップと、

を備えることを特徴とする方法。

【請求項１２】生体情報を用いた認証を行うための照合情報を生成する方法であって、

採取した画像から生体情報を生成するステップと、

外部から提供された情報から識別情報を生成するステップと、

該生体情報と該識別情報とを組み合わせて照合情報を生成するステップと、

を備えることを特徴とする方法。

【請求項１３】生体情報を採取する採取装置から認証を行う認証装置をネッ

トワークで接続した、生体情報を用いた認証システムにおける照合情報生成方法であって、

採取した画像から生体情報を生成するステップと、

採取装置から認証装置にいたる経路情報からなる識別情報を生成するステップと、

該生体情報と該識別情報とを組み合わせて照合情報を生成するステップと、

を備えることを特徴とする方法。

【請求項１４】生体情報を用いた認証方法であって、

生体情報を予め登録してある登録情報と照合するステップと、

生体情報と共に送信されてくる識別情報が所定の条件を満足するかを判定するステップと、

付加情報に写像演算を行うことによって得られる演算値によって識別情報を検証するステップと、

を備えることを特徴とする方法。

【請求項１５】生体情報を用いた認証方法であって、

生体情報を予め登録してある登録情報と照合するステップと、

生体情報と共に送信されてくる識別情報が所定の条件を満足するかを判定するステップと、

を備えることを特徴とする方法。

【請求項１６】生体情報を用いた認証方法であって、

生体情報を取得するステップと、

該生体情報の取得された環境を一意に指定可能な識別情報を取得するステップと、

生体情報と識別情報とを暗号化して送信するステップと、

を備えることを特徴とする方法。

【請求項１７】生体情報を用いた認証を行うための照合情報生成方法をコンピュータに行わせるプログラムを記録した記録媒体であって、該方法は、

生体情報を取得するステップと、

該生体情報を特定可能な識別情報を生成するステップと、

該識別情報を検証可能な付加情報を生成するステップと、

該生体情報と、該識別情報と該付加情報の少なくとも一方とを暗号化し、暗号化された生体情報と付加情報及び、識別情報を組み合わせて照合情報を生成するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

【請求項１８】生体情報を用いた認証を行うための照合情報生成方法をコンピュータに行わせるプログラムを記録した記録媒体であって、該方法は、

採取した画像から生体情報を生成するステップと、

該生体情報生成ステップで生体情報が採取された時刻に関するカウンタ値を取得するステップと

該生体情報と該カウンタ値とを組み合わせて照合情報を生成するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

【請求項１９】生体情報を用いた認証を行うための照合情報生成方法をコンピュータに行わせるプログラムを記録した記録媒体であって、該方法は、

採取した画像から生体情報を生成するステップと、

該生体情報の生成環境を特定する識別情報を生成するステップと

該生体情報と該識別情報とを組み合わせて照合情報を生成するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

【請求項２０】生体情報を用いた認証を行うための照合情報生成方法をコンピュータに行わせるプログラムを記録した記録媒体であって、該方法は、

採取した画像から生体情報を生成するステップと、

外部から提供された情報から識別情報を生成するステップと、

該生体情報と該識別情報とを組み合わせて照合情報を生成するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

【請求項２１】生体情報を採取する採取装置から認証を行う認証装置をネットワークで接続した、生体情報を用いた認証システムにおける照合情報生成方法をコンピュータに行わせるプログラムを記録した記録媒体であって、該方法は、

採取した画像から生体情報を生成するステップと、

採取装置から認証装置にいたる経路情報からなる識別情報を生成するステップ

と、

該生体情報と該識別情報とを組み合わせて照合情報を生成するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

【請求項２２】生体情報を用いた認証方法をコンピュータに実行させるプログラムを記録する記録媒体であって、該方法は、

生体情報を予め登録してある登録情報と照合するステップと、

生体情報と共に送信されてくる識別情報が所定の条件を満足するかを判定するステップと、

付加情報に写像演算を行うことによって得られる演算値によって識別情報を検証するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

【請求項２３】生体情報を用いた認証方法をコンピュータに実行させるプログラムを記録する記録媒体であって、該方法は、

生体情報を予め登録してある登録情報と照合するステップと、

生体情報と共に送信されてくる識別情報が所定の条件を満足するかを判定するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

【請求項２４】生体情報を用いた認証方法をコンピュータに実行させるプログラムを記録する記録媒体であって、該方法は、

生体情報を取得するステップと、

該生体情報の取得された環境を一意に指定可能な識別情報を取得するステップと、

生体情報と識別情報とを暗号化して送信するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、生体情報を用いた認証装置及びその方法に関する。

【０００２】

【従来の技術】

近年、指紋や声紋、虹彩、顔などの生体情報を用いた各種の個人認証装置が販売されている。また、これらの認証装置をネットワーク上で使用し、個人認証システムとしての利用も進んでいる。ネットワーク上での本人認証システムの場合、認証サーバと呼ばれる装置で一括して登録データを管理することが多い。例えば、指紋による本人確認の場合、指紋入力装置を備えたクライアント側で指紋特徴情報を抽出し、サーバに特徴情報を転送する。サーバ側では照合を行い本人として確認した後でアクセス許可などの処理を行う。

【０００３】

これらのシステムのセキュリティを向上するために、生体情報をサーバに転送する場合の秘匿性の確保が重要な課題となっている。

図２６は、従来の生体情報を利用した個人認証システムの構成例を示す図である。

【０００４】

生体情報を利用した個人認証システムの従来のシステムは、被認証者の指紋情報を取得し、暗号化して指紋情報取得時の時刻情報と共にネットワーク３を介してセンタ装置へ送信する端末装置１と、ネットワーク３を介して受信した暗号化された指紋情報と時刻情報とを、登録されている指紋情報を基に解読して受信時刻情報と共に認証判定を行うセンタ装置２とを備えている。

【０００５】

端末装置１の指紋情報取得部１１は、予め設定された場所に指を押印させることによって被認証者の指紋情報を取得する。暗号化部１２は、取得した指紋情報を予め設定された手順によって暗号化する。時計部１３は、第１の実時刻情報を発生する。パケットデータ作成・送信部１４は、暗号化された指紋情報と第１の実時刻情報とをパケットデータに構成して送出する。変調部１５は、ネットワーク３に対応する伝送速度でパケットデータを変調して、回線インターフェース部１６を介してパケットデータをネットワーク３へ送信する。センタ装置２の復調部２２は、ネットワーク３から回線インターフェース部２１を介して受信した変調されたパケットデータを復調する。復調されたパケットデータは、例えば、Ａ

ＴＭネットワークのように、データがセルに分割されて送信されてきた場合などに、パケットデータ受信・組立部２３において、全体が組み立てられ、復元される。暗号復号化部２４では、組み立てられたパケットデータの中の暗号化指紋情報を復号化する。指紋情報登録記憶部２５には、複数の利用者の指紋情報が登録されている。指紋情報解読部２６は、指紋情報登録記憶部２５から登録情報を読み出し、読み出した登録情報と、受信して復号化された指紋情報を照合して、送信されてきた指紋情報が登録情報と一致するか否かを判断する。時計部２７は、第２の実時刻情報を発生する。指紋情報解読部２６で送信されてきた指紋情報が登録情報と一致したと判断された場合に、認証判定部２８は、受信したパケットデータに含まれる第１の実時刻情報と第２の実時刻情報との比較を行って、時刻差が不自然に大きくない場合、受信した指紋情報を認証する。

【０００６】

図２７は、パケットデータの構成を示す図である。

まず、認証を受けようとするユーザは、端末装置１の指紋情報取得部１１の予め設定された位置に指を押印する。指紋情報取得部１１は押印された指の指紋から予め定められた手法によって指紋情報を作成し、暗号化部１２へ送る。暗号化部１２では送られてきた指紋情報を予め設定された手順によって暗号化された指紋情報を作成する。パケットデータ作成・送信部１４では時計部１３からの時刻情報を入手して暗号化部１２からの暗号化された指紋情報と共に、図２７に示すように暗号化指紋情報４１と時刻情報４２とを有するパケットデータ４を作成して送出する。このように、従来の生体情報を用いた認証システムにおいては、生体情報（指紋情報）のみが暗号化されていた。

【０００７】

変調部１５ではネットワーク３に対応した伝送速度でパケット情報を変調して回線インターフェース１６を介してネットワーク３へ送出する。センタ装置２では、復調部２２において、回線インターフェース部２１を介してネットワーク３からの変調されたパケットデータを復調する。

【０００８】

パケットデータ受信・組立部２３では復調されたパケットデータを（ＡＴＭセ

ルなどとして送られてきた場合などに）パケット情報として組み立て、暗号復号化部２４へ送出する。暗号復号化部２４では受信したパケット情報を予め定められた手順に従って元の指紋情報に復号する。

【０００９】

指紋情報解読部２６では指紋情報登録記憶部２５に登録されている複数の指紋情報と受信した指紋情報との照合を行い、一致している指紋情報であれば認証判定部２８に送る。認証判定部２８では、時計部２７が計時する現時刻情報と受信パケットデータに含まれる時刻情報４２との比較を行って、不自然な程の時刻の差異がない（端末装置１とセンタ装置２の各処理時間とネットワーク３での伝送時間の合計した時間は自然な時間と判断する）と判定した場合に、被認証者本人の指紋情報と判定する。この判定の結果、コンピュータセンタ室など、被認証者が認証を受けようとする部分の閉鎖が解かれて、被認証者はコンピュータセンタ室への入室や、金融情報の取得などを行うことが出来るようになる。

【００１０】

このように従来の方法でも被認証者の指紋情報を端末装置１で暗号化して伝送してセンタ装置２でチェックすると共に指紋押印の時刻もチェックするので他人への「なりすまし」等が発生する基となる指紋情報の盗用をある程度は、防止することができる。

【００１１】

一方で、従来の方法では、パケットデータ４の内、暗号化指紋情報４１と時刻情報４２を容易に分離可能であり、時刻情報４２を置換して送付することで「なりすまし」が可能という欠点を有していた。

【００１２】

【発明が解決しようとする課題】

前述のように、上記従来技術によれば、生体情報を用いた個人認証システムにおいて、他人の「なりすまし」を排除する機能が不十分であり、秘匿性の高い情報の保護に対応することが出来ないという問題点があった。

【００１３】

本発明の課題は、生体情報を用いた個人認証システムにおいて、他人の「なり

すまし」などを正確に排除することのできる生体情報を用いた認証装置及び方法を提供することである。

【００１４】

【課題を解決するための手段】

本発明の第１の側面における装置は、生体情報を用いた認証装置において、生体情報を取得する生体情報取得手段と、該生体情報を特定可能な識別情報を生成する識別情報生成手段と、該識別情報を検証可能な付加情報を生成する付加情報生成手段と、該生体情報と該付加情報とを暗号化し、暗号化された生体情報と付加情報及び、識別情報を組み合わせて照合情報を生成する照合情報生成手段とを備えることを特徴とする。

【００１５】

本発明の第２の側面における装置は、生体情報を用いた認証装置であって、生体情報を予め登録してある登録情報と照合する生体情報照合手段と、生体情報と共に送信されてくる識別情報が所定の条件を満足するかを判定する識別情報判定手段と、付加情報に写像演算を行うことによって得られる演算値によって識別情報を検証する識別情報検証手段とを備えることを特徴とする。

【００１６】

本発明の第１の側面における方法は、生体情報を用いた認証を行うための照合情報生成方法であって、生体情報を取得するステップと、該生体情報を特定可能な識別情報を生成するステップと、該識別情報を検証可能な付加情報を生成するステップと、該生体情報と該付加情報とを暗号化し、暗号化された生体情報と付加情報及び、識別情報を組み合わせて照合情報を生成するステップとを備えることを特徴とする。

【００１７】

本発明の第２の側面における方法は、生体情報を用いた認証方法であって、生体情報を予め登録してある登録情報と照合するステップと、生体情報と共に送信されてくる識別情報が所定の条件を満足するかを判定するステップと、付加情報に写像演算を行うことによって得られる演算値によって識別情報を検証するステップとを備えることを特徴とする。

【００１８】

本発明によれば、生体情報と共に、生体情報を特定可能な識別情報と、識別情報が正当なものか否かを検証可能な付加情報とを用いて、送信すべき照合情報とするので、ネットワークを介して照合情報を伝送中に第三者に盗聴されても、第三者が不正な認証要求を行っても、容易に認証することがない。また、第三者には、認証要求に失敗しても、認証されなかったという情報しか得られないので、容易には、認証のために必要な情報を盗むことが出来ない。

【００１９】

更に、照合情報を暗号化すれば、より秘匿性は高まる。

【００２０】

【発明の実施の形態】

本発明によれば、画像として生体情報を採取して認証を行う生体情報を用いた個人認証システムにおいて、採取した画像から生成した生体情報と、生体情報を特定可能な識別情報とによって認証を行うことを特徴とする生体情報を用いた個人認証システムによって、「なりすまし」による生体情報の改ざんを排除する事が可能となり、高いセキュリティを実現するシステムを提供することが可能となる。

【００２１】

本発明は、指紋や音声などの生体情報を用いて個人認証を行う技術に関するもので、生体情報と共に、該生体情報の採取を特定できる情報と共に暗号化したものを照合情報として利用することにより、「なりすまし」に対して高いセキュリティを実現するものである。

【００２２】

図１は、本発明の第１の実施形態において用いる照合情報の構成を説明する図である。

同図において、照合情報５０は、識別情報５１と生体情報５２とで構成されている。生体情報５２は、例えば、指紋画像に含まれる特徴点情報などである。識別情報５１は、生体情報５２の取得が特定可能な情報である。識別情報５１の例としては、生体情報を採取した装置名称あるいは番号や、採取装置から認証を行

うサーバまでの転送ルートを特定可能な情報である。そして、識別情報５１と生体情報５２とを接続し、双方共に暗号化する。このようにすることで、識別情報５１が容易に照合情報５０から分離されることを防止する。また、識別情報５１の内容を、上記例に示したように、悪意の第三者が暗号解読作業中に、容易に、正しい解読結果が得られたと判断できないような情報とする。

【００２３】

図２は、第１の実施形態における照合情報を生成する手順を示したフローチャートである。

まず、ステップＳ１において、生体情報を取得する。例えば、認証を希望するユーザが指紋をセンサに押圧するなどである。次に、ステップＳ２で、識別情報を生成する。これは、前述したように、生体情報を取得した装置の番号など、ユーザの入力とは関係のない、使用した装置などに固有の識別情報とすることが望ましい。そして、ステップＳ３で、生体情報と識別情報を暗号化し、照合情報を生成する。ここで、生体情報と識別情報とを同じ暗号鍵で暗号化しても良いが、生体情報と識別情報とを別々の暗号鍵で暗号化するのも有効である。

【００２４】

図３は、第１の実施形態を実現する装置構成を示した図である。

生体情報入力部１０１は、指紋などの生体情報をセンサから採取する。例えば、画像カメラと画像処理装置及び、画像処理された生体画像から指紋の特徴点情報などの生体情報を抽出する装置とからなる。また、識別情報生成部１０２は、識別情報を生成する。識別情報の内容は、先に示した各種情報を用いることが好ましい。識別情報は、暗号情報生成部１１１において、先の生体情報とともに暗号化され、照合情報生成部２００において、照合情報に変換される。

【００２５】

図４は、図２の手順で生成した照合情報を用いて本人認証を行う手順を示したフローチャートである。

まず、ステップＳ１０において、生体情報と識別情報の暗号を復号する。そして、ステップＳ１１において、生体情報を登録してある情報と照合し、ステップＳ１２において、両者が一致するか否かを判断する。一致しない場合には、ステ

ップＳ１６に進んで、認証しない旨を決定して処理を終了する。ステップＳ１２において、送信されてきた生体情報と登録されている情報とが一致すると判断された場合には、ステップＳ１３に進み、次に、識別情報を照合する。識別情報の照合には、予め使用が許されている装置番号などを登録したデータベースを使う。データベースから登録内容を読み込み、各登録内容と受信した識別情報とをそれぞれ照合することによって、順次照合を行う。あるいは、予め決められた演算を識別情報に施すなどして、決められた結果が得られるか否かなどの判断を行う。ステップＳ１４で、所定の条件が満たされたか、すなわち、装置番号などの照合の場合には、照合の結果、正当な装置による生体情報の採取で悪化と判断されたか否か等、演算を行う場合には、決められた結果が得られたか否か等を判断する。そして、所定の条件を満足した場合には、ステップＳ１５において、認証を行う旨の決定を行って、処理を終了する。ステップＳ１４で、条件が満足されていないと判断された場合には、ステップＳ１６に進んで、認証しないことを決定して処理を終了する。

【００２６】

図５は、図４の処理を行う装置の構成を示した図である。

暗号復号部２１１において、暗号化されている照合情報は、復号され生体情報と識別情報に分離される。分離された情報の内、生体情報は、生体情報照合部２２１において、生体情報格納部２２２に予め登録してある登録情報と照合され、生体情報と登録情報が一致するか否かが判定される。一方の識別情報は、識別情報評価部２２４において、内容が予め設定されている許容範囲を満足するものであるか否かを評価される。予め設定されている許容範囲を満足するとは、例えば、図４のステップＳ１４の説明で述べたこと等を示す。生体情報照合部２２１の生体情報による照合結果と、識別情報評価部２２４における識別情報による評価結果がともに条件を満足するか否かが照合判定部２２３において判断され、満足する場合には、照合情報は認証され、対象者の利用を許可する。利用の許可とは、コンピュータの利用権限の付与等であり、施錠されたドアの開錠などを行う。

【００２７】

本実施形態によれば、生体情報に加えて識別情報による認証も行うので、セキ

ユリティが向上する効果がある。更に、生体情報、識別情報ともに暗号化されているため、第三者による照合情報の解読や置き換えが困難である。従来技術のように暗号化されていない時刻情報が付け替えられる可能性も小さくできる。

【００２８】

図６は、本発明の第２の実施形態の照合情報の構成を示した図である。

本実施形態では、照合情報５５に、図１で示した生体情報５８の採取時あるいは、採取装置などを特定できる識別情報５６に加え、識別情報５６を検証するための付加情報（ＤＤ：ダイジェストデータ）５７を併せて用いる。同図において、付加情報５７と生体情報５８は暗号化されている。付加情報５７と識別情報５６は、以下の関係を満たしており、識別情報５６は付加情報５７を用いて検証可能である。

【００２９】

Ａ＝Ｆ（ＤＤ）　ただし、Ａは識別情報、Ｆは予め定義した写像

この場合、識別情報Ａを先に決定し、逆写像$Ｆ^{-1}$を使って、ＤＤを求める。逆に、ＤＤを先に決定してから、写像Ｆを用いて識別情報Ａを決定しても良い。

【００３０】

照合に用いる照合情報５５は、付加情報５７と生体情報５８に対して、以下の式で表現されるような暗号化を施している。

Ｉ＝Ｈ（Ｂ）　ただし、Ｉは照合情報、Ｂは付加情報と生体情報で構成する情報

本実施形態の構成をとることで、暗号化した照合情報Ｉを他人の情報と置換された場合にも、識別情報Ａを検証することで、その「なりすまし」を検出可能となる。この結果、「なりすまし」に対して、従来以上の高いセキュリティを実現することが可能となる。

【００３１】

本実施形態では、採取した生体情報の特定するための識別情報に加え、識別情報を特定可能な付加情報を生成し、付加情報を生体情報と共に用いることで、改ざんの検出が可能な照合情報を生成することが可能となる。

【００３２】

なお、本実施形態においては、識別情報として、採取時刻を用いることで採取時を特定することが可能である。採取時を識別情報として用いると、識別情報が照合情報から分離され、置き換えられる可能性が残るが、付加情報を使って、識別情報の検証が可能であるので、識別情報が置き換えられたか否かを検証することができる。

【００３３】

また、可変長のパケットを利用した通信システムにおいては、ネットワークの異なる装置を経由する毎に識別情報を付加するようにすることも可能である。

あるいは、識別情報として、生体情報をある装置で採取した順序を特定する順序情報を用いることも可能である。このようにすると、ある装置から送られてくる生体情報が順序情報が示す順番に送られてこない場合、伝送路の途中で何らかの障害あるいは、盗聴が行われたことを検出することが出来る。

【００３４】

識別情報として、採取装置から認証装置にいたる経路情報を用いることも可能である。

図７は、本発明の第３の実施形態の処理手順を示すフローチャートである。

【００３５】

まず、ステップＳ２０において、生体情報を採取する。また、ステップＳ２１において、識別情報を生成する。識別情報は、ステップＳ２０で生体情報を採取した時点で採取時刻あるいは、採取日時、生体情報の採取装置のシリアル番号、カウンタ情報などを取得し、これを用いる。そして、ステップＳ２２で付加情報を生成する。付加情報は、第２の実施形態で説明したように、付加情報の写像が識別情報となるように、照合時点で付加情報に与える写像の逆写像を用いて生成する。そして、ステップＳ２３において、付加情報と生体情報に暗号化処理を施し、ステップＳ２４において、暗号化情報と識別情報とを合わせて、照合情報を生成する。

【００３６】

図８は、第３の実施形態の照合情報生成のための装置構成を示す図である。

図示されていない制御部の指示により、生体情報入力部１０１から、指紋、声

紋、虹彩などの生体情報を取り込み、特徴抽出などにより照合に利用する情報を生成する。この部分は従来例と同様の処理である。生体情報入力部１０１での入力処理とともに、図示されていない制御部の指示により、識別情報生成部１０２において採取時刻の取得あるいは、採取した情報の一連番号など、採取時あるいは採取場所、採取装置などを特定可能な情報を生成する。付加情報生成部１０３において、識別情報を検証可能な付加情報を生成する。このとき、識別情報をそのまま利用することも可能である。暗号情報生成部１１１は、生体情報入力部１０１からの特徴情報と付加情報生成部１０３からの付加情報を暗号化する。

【００３７】

暗号情報生成部１１１で暗号化された情報は、照合情報生成部２００において、識別情報生成部１０２で生成された識別情報と共に、照合情報に変換される

図９は、付加情報の生成手順例を説明するフローチャートである。

【００３８】

なお、同図は、本実施形態の付加情報生成方法を限定するものではなく、例えば、同図以外の方法として、ＭＤ５及びＳＨＡなどの一般的なハッシュ法を用いてもよい。

【００３９】

まず、ステップＳ３０において、ハッシュ値（Ｈ）を“０”に初期化する。次に、ステップＳ３１で、先頭データを処理対象として設定する。ステップＳ３２において、全データの処理が完了したか否かを判断する。全データの処理が完了していない場合には、ステップＳ３３において、計算中のハッシュ値（Ｈ）を８ビット左にシフトする。次に、ステップＳ３４において、ハッシュ値（Ｈ）に処理対象データを加算する。更に、ステップＳ３５において、ハッシュ値（Ｈ）を処理対象の全データサイズで除算する。そして、ステップＳ３６において、次のデータを処理対象として設定し、ステップＳ３２に戻る。ステップＳ３２で、全てのデータの処理が完了したと判断された場合には、ステップＳ３７において、ハッシュ値（Ｈ）で、付加情報の生成が完了したとして、処理を終了する。

【００４０】

図１０は、第３の実施形態において、照合を実行する手順を示すフローチャー

トである。

まず、ステップＳ４０において、受信した照合情報から暗号情報と識別情報に分離した後、ステップＳ４１において、暗号化された情報を復号し、生体情報と付加情報に分離する。ステップＳ４２において、生体情報を予め登録してある登録情報と照合し、ステップＳ４３において、一致しているか否かを判断する。ステップＳ４３において、生体情報と登録情報とが一致していないと判断された場合には、ステップＳ４７において、認証しないと判定し処理を終了する。ステップＳ４３において、生体情報と登録情報とが一致していると判断された場合には、ステップＳ４４において、付加情報から識別情報の検証用情報を生成する。例えば、付加情報に予め定められていた写像を施して検証用情報を生成する。あるいは、付加情報が図９の処理によって生成された場合には、図９の処理の逆処理を行って検証用情報を生成する。

【００４１】

ステップＳ４５において、生成された検証情報と、照合情報から分離した識別情報を比較し、識別情報を検証する。識別情報が、検証情報で検証された場合、ステップＳ４６において、本人として認証を行う。識別情報が検証情報で検証されなかった場合には、ステップＳ４７において、認証を行わないことを決定して処理を終了する。

【００４２】

本実施形態の場合、最終的に生体情報を入力した人物に通知されるのは、本人として認証したか否かの結果だけである。「なりすまし」を成功させるには、暗号の解読と付加情報からの検証情報生成方法の解読が必要であるが、認証したか否かだけの情報では、これらの解読を十分行うことが出来ないので、従来例で示した方法に比べ、格段に秘匿性が向上する。

【００４３】

図１１は、第３の実施形態における照合部の構成を示した図である。

照合情報は、照合情報分離部２０１で、生体情報と付加情報で構成される暗号情報と識別情報に分離される。暗号復号部２１１において、暗号情報が復号された後、生体情報は生体情報照合部２２１において、生体情報格納部２２２に予め

格納してある生体情報と照合され、結果を照合判定部２２３に通知する。付加情報は、付加情報格納部２１３に格納された後、識別情報検証部２１４で識別情報格納部２１２内の識別情報を検証するのに使用される。検証結果は、識別情報検証部２１４から、照合判定部２２３に通知される。照合判定部２２３では、生体情報照合部２２１と識別情報検証部２１４からの通知がともに「認証」の場合のみ、照合結果として「認証」を出力する。

【００４４】

図１２は、本発明の第４の実施形態を照合情報生成手順を示すフローチャートである。

本実施形態では、指紋採取時の装置内蔵のカウンタ情報を取得し、識別情報としている。その後、指紋採取時のカウンタ情報からダイジェスト情報（付加情報）を生成する。採取した指紋画像から特徴点を抽出した生体情報とダイジェスト情報を暗号化した後、採取カウンタ情報で構成する識別情報と共に、通信部を経て、ネットワーク上の認証サーバに送信する。その後、認証サーバからの認証結果を、ネットワークを介して通信部で受信して、一連の認証処理を終了する。

【００４５】

まず、照合情報生成手順においては、ステップＳ５０において、指紋画像の採取を行う。次に、ステップＳ５１で、指紋画像を採取した時点でのカウンタの値であるカウンタ情報を取得する。ステップＳ５２において、カウンタ情報からダイジェスト情報を生成し、ステップＳ５３において、指紋特徴点とダイジェスト情報を暗号化する。そして、ステップＳ５４において、カウンタ情報と暗号データから照合情報を生成する。ステップＳ５５において、ネットワークを介して認証サーバに照合情報を送信し、ステップＳ５６において、ネットワークを介して認証サーバの認証結果を受信する。

【００４６】

図１３は、第４の実施形態の照合情報を生成する端末装置の構成を説明する図である。

指紋画像採取部１３１で指紋画像を採取すると共に、特徴点情報を抽出する。図示していない制御部の指示により、指紋画像採取時のカウンタ更新部１３４の

カウンタ情報をカウンタ情報取得部１３３で記録し、ダイジェスト生成部１３２で、検証用情報を生成する。生成されたダイジェスト情報と前記指紋画像採取部１３１で採取されて抽出された特徴点情報は、暗号情報生成部１１１で暗号化される。先のカウンタ情報取得部１３３で記録した採取カウンタ情報は、識別情報として照合情報生成部１２１で、暗号情報生成部１１１からの暗号情報と合成され、通信部１５０を経て、図示していないネットワークを介して認証サーバに送信される。認証サーバによる認証結果は、通信部１５０で受信する。

【００４７】

図１４は、第４の実施形態の照合を行う手順を説明するフローチャートである。

認証サーバでは、ステップＳ６０において通信部で照合情報を受信した後、ステップＳ６１において、暗号情報と識別情報に分離する。暗号情報は、ステップＳ６２において、復号され、生体情報（指紋の特徴点情報）とカウンタ情報検証用のダイジェスト情報とに分離される。ステップＳ６３で、指紋の特徴点情報を予め登録してある情報と照合する。ステップＳ６４において、照合の結果が一致か不一致かが判定され、不一致の場合には、ステップＳ７０において、認証しない旨決定し、この決定をステップＳ７１において、ネットワークに送信する。ステップＳ６４において、照合の結果、特徴点情報と登録情報が一致している場合には、ステップＳ６５において、採取時のカウンタ情報と現カウンタ情報を比較する。ステップＳ６６で、カウンタの比較結果が所定の時間差であれば、ダイジェストを用いて、識別情報として分離されている採取時のカウンタ情報を検証する（ステップＳ６７）。ステップ６８で、ダイジェスト情報と採取カウンタ情報との比較の結果、一致していないと判断された場合には、ステップＳ７０に進み、ステップＳ７０において、認証しない旨決定し、結果をネットワークに送信する（ステップＳ７１）。ステップＳ６８において、検証の結果、一致が確認された場合、ステップＳ６９において、認証すべき旨決定し、通信部から、「認証」したとして結果を送信する（ステップＳ７１）。

【００４８】

図１５は、第４の実施形態の照合部の構成を説明する図である。

先の図１１に比べ、カウンタ計測部２３２と採取カウンタ情報比較部２３７が加えられている。

【００４９】

照合情報を受信した通信部２５０は、これを照合情報分離部２０１に入力する。照合情報分離部２０１では、照合情報から、暗号情報とカウンタ情報を分離する。暗号情報は、暗号復号部２１１において復号され、生体情報とダイジェスト情報とに分離される。そして、生体情報は、生体情報照合部２３４において、生体情報格納部２３３に格納されている登録情報と照合され、結果が照合判定部２３８に送られる。一方、ダイジェスト情報は、ダイジェスト解読部２３５に入力され、ダイジェスト情報から、カウンタ情報が、写像演算によって求められる。

【００５０】

また、照合情報分離部２０１において、分離された採取カウンタ情報は、採取カウンタ情報格納部２３１に一旦格納された後、ダイジェスト比較部２３６において、ダイジェスト解読部２３５において得られたカウンタ値と比較され、結果が照合判定部２３８に入力される。また、採取カウンタ情報は、採取カウンタ情報比較部２３７において、カウンタ計測部２３２のカウンタ値と比較され、採取カウンタ情報とカウンタ値の差が、所定の範囲に入っているか否かを判定し、照合判定部２３８に入力される。

【００５１】

照合判定部２３８では、生体情報の一致が得られ、ダイジェスト情報による採取カウンタ情報の比較の結果が一致し、かつ、採取カウンタ情報と、カウンタ計測部２３２との差が一定値以内である場合に、照合情報の照合結果が一致したと判断する。

【００５２】

同図の実施例では、内蔵型カウンタを利用する形態を示した。この場合、各装置間のカウンタ情報の整合性を確保する方法としては、以下の方法がある。つまり、各装置にインストールするソフトウェアの制作時の時刻情報を起点として、インストール時に、各装置の時刻情報と起点とする時刻との差を、利用するカウンタの刻みに換算して、初期値を確定する。その後は、所定の時間間隔（認証で

許容する時間範囲を単位）として、各装置内のカウンタをカウントアップする。こうして、各装置間でのカウンタ値の整合性を確保することが可能となる。

【００５３】

また、カウンタを各装置の内蔵カウンタとせず、ネットワーク内に設置された装置からの共通のカウンタ情報を通信回線などを経由して取得する構成とすることが可能である。

【００５４】

図１６は、共通カウンタ情報を通信回線を経由して端末装置が取得する実施形態の概略構成図である。

端末装置３１０－１と３１０－２は、いずれかが生体情報採取装置であり、他方が指紋などの生体情報を照合する照合装置である。共通カウンタ装置１００は、端末装置３１０－１と３１０－２が共通に使用するカウンタ値を供給するカウンタ装置である。例えば、端末装置３１０－１が生体情報採取装置であるとすると、端末３１０－１は、生体情報を採取し、照合情報を作成する場合に、共通カウンタ装置１００からカウンタ値をネットワークＡを介して取得して、照合情報のカウンタ情報を生成する。端末３１０－１から送信された照合情報は、ネットワークＡを介して、端末装置３１０－２に送られる。端末装置３１０－２では、受信した照合情報を第４の実施形態のように、処理し、カウンタ情報の照合を行う。ここで、第４の実施形態においては、送信側と同期した内臓のカウンタを用いてカウンタ値を取得し、カウンタ値の比較を行っていたが、本実施形態では、共通カウンタ装置１００からネットワークＡを介してカウンタ値を取得して、照合情報に含まれていたカウンタ値と比較する。

【００５５】

このようにすることによって、内臓のカウンタを使用する場合のように、送信側と受信側のカウンタを同期させておく必要が無く、より装置構成を簡単化できる。

【００５６】

図１７は、第５の実施形態のデータ構造を説明する図である。

本実施形態のデータは、指紋データ（生体情報）と指紋データを認証するまで

に経由する経路情報で構成する。

【００５７】

すなわち、まず、同図（１）に示されるように、照合情報を送信する場合には、送信装置は、生体情報である指紋データと指紋データに基づいて生成された付加情報（判定基準情報）ａ０を生成し、双方を暗号化して、１つのパケットとして送出する。次に、ルート１に存在する中継器をこの照合情報が通過すると、中継器は、この照合情報に、ルート１を特定する識別子と、この識別子の写像（この場合、判定基準情報ａ０を使用する）を使って作成した付加情報ａ１とを（１）のパケットに添付して、（２）のようなパケットデータを送出する。更に、（２）のパケットがルート２に存在する中継器を通過すると、この中継器は、ルート２を特定する識別子と、この識別子の写像を使って作成した付加情報ａ２を（２）のパケットに添付し、付加情報ａ１を取り除いて（３）のパケットを生成し、送出する。

【００５８】

このように、ネットワークの特定のルートに存在する中継器が、照合情報が通過する度に、ルートに関する情報をパケットに添付することにより、照合情報が、不自然なルートを通ったか否か、あるいは、正規のルートを通って来たか否かを判断することが出来る。

【００５９】

図１８は、第５の実施形態のシステム構成を説明する図である。

端末装置３１０と認証装置３３０との間に、一台以上の中継装置３２０が介在する構成となっている。

【００６０】

端末装置３１０は、採取した生体情報を基に、照合情報を生成して、ネットワークＡに送出する。中継装置３２０は、ネットワークＡから照合情報を受信すると、中継器３２０の存在するルートの識別子あるいは識別情報を照合情報に添付し、更に、識別子あるいは識別情報から生成した付加情報も図１７で説明したように照合情報に添付して、ネットワークＢに送出する。認証装置３３０は、ネットワークＢから照合情報を受信すると、生体情報の照合をすると共に、識別情報

の照合、及び、識別情報が改ざんされていないかを付加情報を使って検証し、端末装置３１０を使って認証を求めてきたユーザを認証するか否かを判断する。判断結果は、ネットワークＢ、中継装置３２０、ネットワークＡを介して、端末装置３１０に送られる。

【００６１】

判定基準値及び付加情報の生成方法は図９と同様なので説明を省略する。ただし、図９は、あくまでも例であり、作成方法を特に定めるものではない。図９以外の方法として、ＭＤ５及びＳＨＡなどの一般的なハッシュ法を用いてもかまわない。ここで、判定基準値とは、図１７のａ０のことであって、生体情報に基づいた付加情報を意味する。

【００６２】

図１９は、図１８の端末装置３１０が行う処理手順を示すフローチャートである。

まず、ステップＳ７５において、指紋画像の採取を行い、ステップＳ７６において、指紋データの判定基準値を算出する。次に、ステップＳ７７において、指紋データと指紋データの判定基準値を暗号化して、照合情報を生成する。そして、ステップＳ７８で、ネットワークを介して照合情報を中継装置に送信する。

【００６３】

なお、ここで、生体情報として指紋データを説明したが、上記処理は一般の生体情報に適用が可能である。

図２０は、端末装置３１０の装置構成を説明する図である。

【００６４】

端末装置３１０では、指紋画像採取部１３１で指紋画像を採取し、指紋情報を抽出する。そして、判定基準値生成部３１１において、採取指紋情報から認証装置３３０による認証時に判定基準値となる一方向写像値を算出し、暗号情報生成部３１２において、一方向写像値と採取指紋情報を暗号化した後、通信部３５１を経て、ネットワーク上の中継装置に送信する。判定基準値は以下の式で生成され、暗号化される。

【００６５】

ａ０＝H_0（指紋データ）

図２１は、中継装置３２０の処理手順を説明するフローチャートである。

まず、ステップＳ８０で、ネットワークから照合情報を受信する。次に、ステップＳ８１で、照合情報から直前の中継装置の写像値を認識する。そして、ステップＳ８２において、自中継装置のダイジェストを算出する。そして、ステップＳ８３において、直前の中継装置の写像値と自中継装置のダイジェストから自中継装置を示す写像値を算出する。ステップＳ８４において、写像値の置き換えを行い、ステップＳ８５において、通信データの先頭に自中継装置の情報を付加し、ステップＳ８６において、照合情報をネットワークに送信する。

【００６６】

図２２は、中継装置３２０の装置構成を説明する図である。

本実施形態の場合、中継装置３２０を経由する際に、中継装置３２０を特定可能な情報を指紋データに付加していくことにより、ネットワーク内の伝送途中で、データを差し替えられることを防止するものである。付加情報は、以下の式で生成され、中継装置識別情報と共に、非暗号化部として付加される。

【００６７】

ａ１＝H_{a0}（Ｄ（route　1））

ａ２＝H_{a1}（Ｄ（route　2））

・

・

・

・

ａｎ＝$H_{a(n-1)}$（Ｄ（route　n））

route　nで示した情報は、中継装置３２０を特定するための情報であり、ネットワーク内のＩＰアドレス情報などがこれにあたる。更に、中継装置３２０に指紋データが到達した時刻を取得し、ＩＰアドレス情報と共にroute　nとして、直前の中継装置などで付加されたデータａ（ｎ－１）を用いた一方向写像値をａｎとして、付加する。

【００６８】

通信部３５１は、照合情報を受信すると、これを照合情報分離部３２１に入力する。照合情報分離部３２１は、受信した照合情報から、暗号化された情報と、暗号化されていない情報とを分離し、それぞれ暗号化情報格納部３２２と非暗号情報格納部３２３に入力する。暗号情報格納部３２２に格納された暗号情報は、適当なタイミングで読み出され、照合情報生成部３２６に入力される。一方、非暗号情報は、非暗号情報格納部３２３から読み出された後、ダイジェスト生成部３２５に入力される。また、ダイジェスト生成部３２５には、中継器のＩＰアドレスなどを取得する装置情報取得部３２４から、ＩＰアドレスなどの装置情報が入力される。ダイジェスト生成部３２５は、非暗号情報と装置情報とから、上述したような手順で、ダイジェストを生成し、照合情報生成部３２６に入力する。照合情報生成部３２６は、暗号情報とダイジェスト情報とから、照合情報を生成し、通信部３５２を介してネットワークに送出する。

【００６９】

図２３は、第５の実施形態における認証装置３３０の動作手順を説明するフローチャートである。

まず、ステップＳ９０において、ネットワークから照合情報を受信する。次に、ステップＳ９１において、照合情報を暗号情報と中継装置付加情報に分離する。ステップＳ９２において、暗号を復号し、生体情報と判定基準値に分離し、ステップＳ９３において、指紋情報を登録してある情報と照合する。ステップＳ９４において、指紋情報と登録情報とが一致するか否かを判断し、一致しない場合には、ステップＳ９９で、認証しないことを決定し、ステップＳ１００において、認証結果をネットワークに送信する。

【００７０】

ステップＳ９４で、指紋情報と登録情報とが一致すると判断した場合には、ステップＳ９５において、中継装置付加情報から判定基準値を算出する。そして、ステップＳ９６において、算出した判定基準値と復号した判定基準値とを比較し、ステップＳ９７において、両者が一致するか否かを判断する。両者が一致しない場合には、ステップＳ９９において、認証しない旨を決定し、ステップＳ１００において、認証結果をネットワークに送信する。ステップＳ９７において、両

者が一致したと判断した場合には、ステップＳ９８において、認証する旨を決定し、ステップＳ１００において、認証結果をネットワークに送信する。

【００７１】

なお、ここでは、中継装置付加情報から判定基準値を算出し、復号された判定基準値と比較しているが、中継付加情報から判定基準値を算出する写像の逆写像が存在する場合には、復号した判定基準値から中継装置付加情報を逆写像によって求め、復号した中継装置付加情報と算出した中継装置付加情報とを比較しても良い。

【００７２】

図２４は、第５の実施形態の認証装置３３０の装置構成を説明する図である。

認証装置３３０では、通信部３５２において照合情報を受信した後、照合情報分離部３２１において暗号情報と中継装置付加情報に分離する。暗号情報は、暗号復号部３３１において復号されて生体情報（例えば、指紋の特徴点情報）と判定基準値に分離され、該生体情報は、生体情報照合部２３４において指紋の特徴点情報を予め登録してある生体情報格納部２３３の登録情報と照合される。

【００７３】

また、判定基準値解析部３３２は、中継装置付加情報から判定基準値を算出し、判定基準値比較部３３３において、復号した判定基準値と比較される。そして、照合判定部３３４は、生体情報の照合結果と判定基準値の照合結果がいずれも一致している場合に、「認証」したとして認証結果をネットワークへ送信する。上記いずれかの照合あるいは比較、検証が条件を満足しない場合、「認証せず」として認証結果をネットワークへ送信する。

【００７４】

図２５は、上記実施形態をソフトウェアで実現する場合に必要となるハードウェア構成を説明する図である。

本発明の実施形態をソフトウェア（プログラム）で実現する場合、プログラムの実行装置は、ＣＰＵ４０１にバス４００を介して接続された各装置から構成される。ＲＯＭ４０２は、ＢＩＯＳなどを格納し、装置が電源投入されると、ＣＰＵ４０１からＲＯＭ４０２にアクセスが生じ、ＣＰＵ４０１がＢＩＯＳを読み込

んで、各装置の制御を可能とする。ＲＯＭ４０２には、本発明の実施形態を実現するプログラムを記憶させておくことが可能である。このようにすると、プログラムを電源投入と同時に実行することが出来、装置を生体情報の照合情報生成装置あるいは、照合情報の照合装置専用の装置として使用することが出来る。

【００７５】

また、当該プログラムは、ハードディスクなどの記憶装置４０７に記憶しておき、必要に応じてＲＡＭ４０３に展開して、ＣＰＵ４０１が実行可能とすることも可能である。あるいは、当該プログラムを可搬記録媒体４０９に記録して持ち運び可能とし、必要に応じて、記録媒体読み取り装置４０８で、可搬記録媒体４０９に記録されているプログラムをＲＡＭ４０３に読み込み、ＣＰＵ４０１が実行するようにしても良い。また、可搬記録媒体４０９に記録されたプログラムを一旦記憶装置４０７に記憶してからＣＰＵ４０１が実行するようにしても良い。

【００７６】

あるいは、通信インターフェース４０４を使って、ネットワーク４０５に接続し、情報提供者４０６から当該プログラムをダウンロードして実行することも可能である。また、図１６などで説明したように、生体情報採取装置と照合装置をネットワーク４０５で接続して使用する場合には、例えば、情報提供者４０６を照合装置と見なすこともでき、その場合、同図の装置は、照合情報の生成を行い、情報提供者４０６に照合情報を送って、認証結果を受け取る処理を行うことになる。また、同図の装置と情報提供者４０６の役割を逆転することも可能である。更に、当該プログラムをネットワーク４０５を介してダウンロードするのではなく、ネットワーク環境下でダウンロードせずに実行することも可能である。

【００７７】

入出力装置は、通常、キーボード、マウス、ディスプレイ等からなるが、同図の装置を生体情報採取装置として使用する場合には、生体情報を採取するためのセンサが必要になる。また、ディスプレイには、認証結果、すなわち、ユーザを認証するかしないかの表示を行う。更に、重要なデータを扱うコンピュータ室への入出許可の認証を行うような場合には、入出力装置に、コンピュータ室の施錠、開錠を行う機構等も含まれる。

＜付記＞

本発明は、以下の形態でも実施が可能である。

１．生体情報を用いた認証装置において、

生体情報を取得する生体情報取得手段と、

該生体情報を特定可能な識別情報を生成する識別情報生成手段と、

該識別情報を検証可能な付加情報を生成する付加情報生成手段と、

該生体情報と、該識別情報と該付加情報の少なくとも一方とを暗号化し、暗号化された生体情報と付加情報及び、識別情報を組み合わせて照合情報を生成する照合情報生成手段と、

を備えることを特徴とする装置。

２．前記付加情報と、生体情報とを暗号化することを特徴とする１に記載の装置。

３．前記識別情報として、生体情報の採取時刻を用いることを特徴とする１に記載の装置。

４．前記識別情報は、異なる装置を経由する毎に識別情報を付加されることを特徴とする１に記載の装置。

５．前記生体情報に前記識別情報を付加する際に、前記付加情報を該識別情報の検証のための情報とし、前記識別情報が付加される毎に新たな付加情報を生成して、前記照合情報に付加することを特徴とする４に記載の装置。

６．生体情報を用いた認証装置において、

採取した画像から生体情報を生成する生体情報生成手段と、

該生体情報生成手段に内蔵された、生体情報の採取時刻に関するカウンタ値をカウントするカウンタ手段と

該生体情報と該カウンタ手段のカウンタ値とを組み合わせて照合情報を生成する照合情報生成手段と、

を備えることを特徴とする装置。

７．生体情報を用いた認証装置において、

採取した画像から生体情報を生成する生体情報生成手段と、

該生体情報生成手段を特定する識別情報と、該生体情報生成手段内で生成した

生体情報の採取順序を特定する順序情報の少なくともいずれか一方からなる識別情報を生成する識別情報生成手段と

該生体情報と該識別情報とを組み合わせて照合情報を生成する照合情報生成手段と、

を備えることを特徴とする装置。

８．生体情報を用いた認証装置において、

採取した画像から生体情報を生成する生体情報生成手段と、

外部から提供された情報から識別情報を生成する識別情報生成手段と、

該生体情報と該識別情報とを組み合わせて照合情報を生成する照合情報生成手段と、

を備えることを特徴とする装置。

９．生体情報を採取する採取装置から認証を行う認証装置をネットワークで接続した、生体情報を用いた認証システムにおいて、

採取した画像から生体情報を生成する生体情報生成手段と、

採取装置から認証装置にいたる経路情報からなる識別情報を生成する識別情報生成手段と、

該生体情報と該識別情報とを組み合わせて照合情報を生成する照合情報生成手段と、

を備えることを特徴とする装置。

１０．生体情報と識別情報とを暗号化することを特徴とする６～９のいずれか１つに記載の装置。

１１．生体情報を用いた認証装置であって、

生体情報を予め登録してある登録情報と照合する生体情報照合手段と、

生体情報と共に送信されてくる識別情報が所定の条件を満足するかを判定する識別情報判定手段と、

付加情報に写像演算を行うことによって得られる演算値によって識別情報を検証する識別情報検証手段と、

を備えることを特徴とする装置。

１２．生体情報を用いた認証装置であって、

生体情報を予め登録してある登録情報と照合する生体情報照合手段と、

生体情報と共に送信されてくる識別情報が所定の条件を満足するかを判定する識別情報判定手段と、

を備えることを特徴とする装置。

１３．生体情報を用いた認証装置であって、

生体情報を取得する生体情報取得手段と、

該生体情報の取得された環境を一意に指定可能な識別情報を取得する識別情報取得手段と、

生体情報と識別情報とを暗号化して送信する暗号化・送信手段と、

を備えることを特徴とする装置。

１４．生体情報を用いた認証を行うための照合情報生成方法であって、

生体情報を取得するステップと、

該生体情報を特定可能な識別情報を生成するステップと、

該識別情報を検証可能な付加情報を生成するステップと、

該生体情報と、該識別情報と該付加情報の少なくとも一方とを暗号化し、暗号化された生体情報と付加情報及び、識別情報を組み合わせて照合情報を生成するステップと、

を備えることを特徴とする方法。

１５．前記付加情報と、生体情報とを暗号化することを特徴とする１４に記載の方法。

１６．前記識別情報として、生体情報の採取時刻を用いることを特徴とする１４に記載の方法。

１７．前記識別情報は、異なる装置を経由する毎に識別情報を付加されることを特徴とする１４に記載の方法。

１８．前記生体情報に前記識別情報を付加する際に、前記付加情報を該識別情報の検証のための情報とし、前記識別情報が付加される毎に新たな付加情報を生成して、前記照合情報に付加することを特徴とする１７に記載の方法。

１９．生体情報を用いた認証を行うための照合情報を生成する方法であって、

採取した画像から生体情報を生成するステップと、

該生体情報生成ステップで生体情報が採取された時刻に関するカウンタ値を取得するステップと

該生体情報と該カウンタ値とを組み合わせて照合情報を生成するステップと、を備えることを特徴とする方法。

２０．生体情報を用いた認証を行うための照合情報を生成する方法であって、

採取した画像から生体情報を生成するステップと、

該生体情報の生成環境を特定する識別情報を生成するステップと

該生体情報と該識別情報とを組み合わせて照合情報を生成するステップと、を備えることを特徴とする方法。

２１．生体情報を用いた認証を行うための照合情報を生成する方法であって、

採取した画像から生体情報を生成するステップと、

外部から提供された情報から識別情報を生成するステップと、

該生体情報と該識別情報とを組み合わせて照合情報を生成するステップと、を備えることを特徴とする方法。

２２．生体情報を採取する採取装置から認証を行う認証装置をネットワークで接続した、生体情報を用いた認証システムにおける照合情報生成方法であって、

採取した画像から生体情報を生成するステップと、

採取装置から認証装置にいたる経路情報からなる識別情報を生成するステップと、

該生体情報と該識別情報とを組み合わせて照合情報を生成するステップと、を備えることを特徴とする方法。

２３．生体情報と識別情報とを暗号化することを特徴とする１９～２２のいずれか１つに記載の方法。

２４．生体情報を用いた認証方法であって、

生体情報を予め登録してある登録情報と照合するステップと、

生体情報と共に送信されてくる識別情報が所定の条件を満足するかを判定するステップと、

付加情報に写像演算を行うことによって得られる演算値によって識別情報を検証するステップと、

を備えることを特徴とする方法。

２５．生体情報を用いた認証方法であって、

生体情報を予め登録してある登録情報と照合するステップと、

生体情報と共に送信されてくる識別情報が所定の条件を満足するかを判定するステップと、

を備えることを特徴とする方法。

２６．生体情報を用いた認証方法であって、

生体情報を取得するステップと、

該生体情報の取得された環境を一意に指定可能な識別情報を取得するステップと、

生体情報と識別情報とを暗号化して送信するステップと、

を備えることを特徴とする方法。

２７．生体情報を用いた認証を行うための照合情報生成方法をコンピュータに行わせるプログラムを記録した記録媒体であって、該方法は、

生体情報を取得するステップと、

該生体情報を特定可能な識別情報を生成するステップと、

該識別情報を検証可能な付加情報を生成するステップと、

該生体情報と、該識別情報と該付加情報の少なくとも一方とを暗号化し、暗号化された生体情報と付加情報及び、識別情報を組み合わせて照合情報を生成するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

２８．生体情報を用いた認証を行うための照合情報生成方法をコンピュータに行わせるプログラムを記録した記録媒体であって、該方法は、

採取した画像から生体情報を生成するステップと、

該生体情報生成ステップで生体情報が採取された時刻に関するカウンタ値を取得するステップと

該生体情報と該カウンタ値とを組み合わせて照合情報を生成するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

２９．生体情報を用いた認証を行うための照合情報生成方法をコンピュータに行

わせるプログラムを記録した記録媒体であって、該方法は、

採取した画像から生体情報を生成するステップと、

該生体情報の生成環境を特定する識別情報を生成するステップと

該生体情報と該識別情報とを組み合わせて照合情報を生成するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

３０．生体情報を用いた認証を行うための照合情報生成方法をコンピュータに行わせるプログラムを記録した記録媒体であって、該方法は、

採取した画像から生体情報を生成するステップと、

外部から提供された情報から識別情報を生成するステップと、

該生体情報と該識別情報とを組み合わせて照合情報を生成するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

３１．生体情報を採取する採取装置から認証を行う認証装置をネットワークで接続した、生体情報を用いた認証システムにおける照合情報生成方法をコンピュータに行わせるプログラムを記録した記録媒体であって、該方法は、

採取した画像から生体情報を生成するステップと、

採取装置から認証装置にいたる経路情報からなる識別情報を生成するステップと、

該生体情報と該識別情報とを組み合わせて照合情報を生成するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

３２．生体情報を用いた認証方法をコンピュータに実行させるプログラムを記録する記録媒体であって、該方法は、

生体情報を予め登録してある登録情報と照合するステップと、

生体情報と共に送信されてくる識別情報が所定の条件を満足するかを判定するステップと、

付加情報に写像演算を行うことによって得られる演算値によって識別情報を検証するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

３３．生体情報を用いた認証方法をコンピュータに実行させるプログラムを記録する記録媒体であって、該方法は、

生体情報を予め登録してある登録情報と照合するステップと、

生体情報と共に送信されてくる識別情報が所定の条件を満足するかを判定するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

３４．生体情報を用いた認証方法をコンピュータに実行させるプログラムを記録する記録媒体であって、該方法は、

生体情報を取得するステップと、

該生体情報の取得された環境を一意に指定可能な識別情報を取得するステップと、

生体情報と識別情報とを暗号化して送信するステップと、

を備えることを特徴とする、コンピュータ読み取り可能な記録媒体。

【００７８】

【発明の効果】

本発明による生体情報を用いた認証システムにより、「なりすまし」による生体情報の改ざんを排除することが可能となり、高いセキュリティを実現するシステムを提供することが可能となる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態において用いる照合情報の構成を説明する図である。

【図２】

第１の実施形態における照合情報を生成する手順を示したフローチャートである。

【図３】

第１の実施形態を実現する装置構成を示した図である。

【図４】

図２の手順で生成した照合情報を用いて本人認証を行う手順を示したフローチャートである。

【図５】

図４の処理を行う装置の構成を示した図である。

【図６】

本発明の第２の実施形態の照合情報の構成を示した図である。

【図７】

本発明の第３の実施形態の処理手順を示すフローチャートである。

【図８】

第３の実施形態の照合情報生成のための装置構成を示す図である。

【図９】

付加情報の生成手順例を説明するフローチャートである。

【図１０】

第３の実施形態において、照合を実行する手順を示すフローチャートである。

【図１１】

第３の実施形態における照合部の構成を示した図である。

【図１２】

本発明の第４の実施形態を照合情報生成手順を示すフローチャートである。

【図１３】

第４の実施形態の照合情報を生成する端末装置の構成を説明する図である。

【図１４】

第４の実施形態の照合を行う手順を説明するフローチャートである。

【図１５】

第４の実施形態の照合部の構成を説明する図である。

【図１６】

共通カウンタ情報を通信回線を経由して端末装置が取得する実施形態の概略構成図である。

【図１７】

第５の実施形態のデータ構造を説明する図である。

【図１８】

第５の実施形態のシステム構成を説明する図である。

【図１９】

図１８の端末装置３１０が行う処理手順を示すフローチャートである。

【図２０】

端末装置３１０の装置構成を説明する図である。

【図２１】

中継装置３２０の処理手順を説明するフローチャートである。

【図２２】

中継装置３２０の装置構成を説明する図である。

【図２３】

第５の実施形態における認証装置３３０の動作手順を説明するフローチャートである。

【図２４】

第５の実施形態の認証装置３３０の装置構成を説明する図である。

【図２５】

上記実施形態をソフトウェアで実現する場合に必要となるハードウェア構成を説明する図である。

【図２６】

従来の生体情報を利用した個人認証システムの構成例を示す図である。

【図２７】

従来のパケットデータの構成を示す図である。

【符号の説明】

５０、５５　照合情報

５１、５６　識別情報

５２、５８　生体情報

５７　付加情報（ダイジェストデータ）

１００　共通カウンタ装置

１０１　生体情報入力部

１０２　識別情報生成部

１０３　付加情報生成部

１１１　暗号情報生成部

１２１　照合情報生成部

１３１　　指紋画像採取部

１３２　　ダイジェスト生成部

１３３　　カウンタ情報取得部

１３４　　カウンタ更新部

１５０、２５０、３５１、３５２　　通信部

２００　　照合情報生成部

２０１、３２１　　照合情報分離部

２１１　　暗号復号部

２１２　　識別情報格納部

２１３　　付加情報格納部

２１４　　識別情報検証部

２２１　　生体情報照合部

２２２　　生体情報格納部

２２３、２３８　　照合判定部

２３１　　採取カウンタ情報格納部

２３２　　カウンタ計測部

２３３　　生体情報格納部

２３４　　生体情報照合部

２３５　　ダイジェスト解説部

２３６　　ダイジェスト比較部

２３７　　採取カウンタ情報比較部

３１１　　判定基準値生成部

３１２　　暗号情報生成部

３１０－１、３１０－２、３１０　　端末装置

３２０　　中継装置

３３０　　認証装置

３２２　　暗号情報格納部

３２３　　非暗号情報格納部

３２４　　装置情報取得部

３２５　　ダイジェスト生成部

３２６　　照合情報生成部

３３１　　暗号復号部

３３２　　判定基準値解析部

３３３　　判定基準値比較部

３３４　　生体情報照合部

３３４　　照合判定部

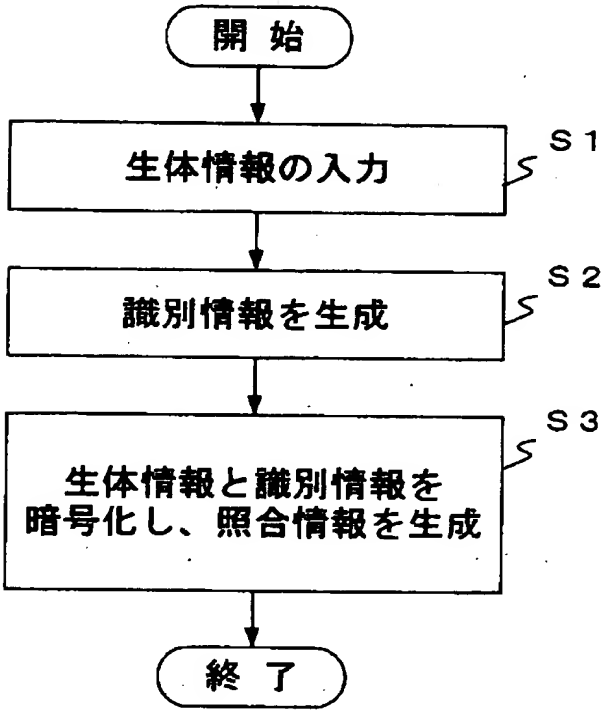
【書類名】　　図面

【図１】

本発明の第１の実施形態において用いる
照合情報の構成を説明する図

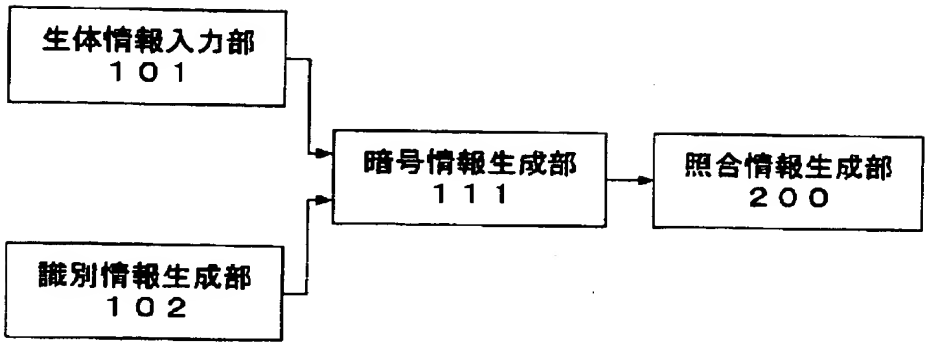
【図２】

第１の実施形態における照合情報を
生成する手順を示したフローチャート



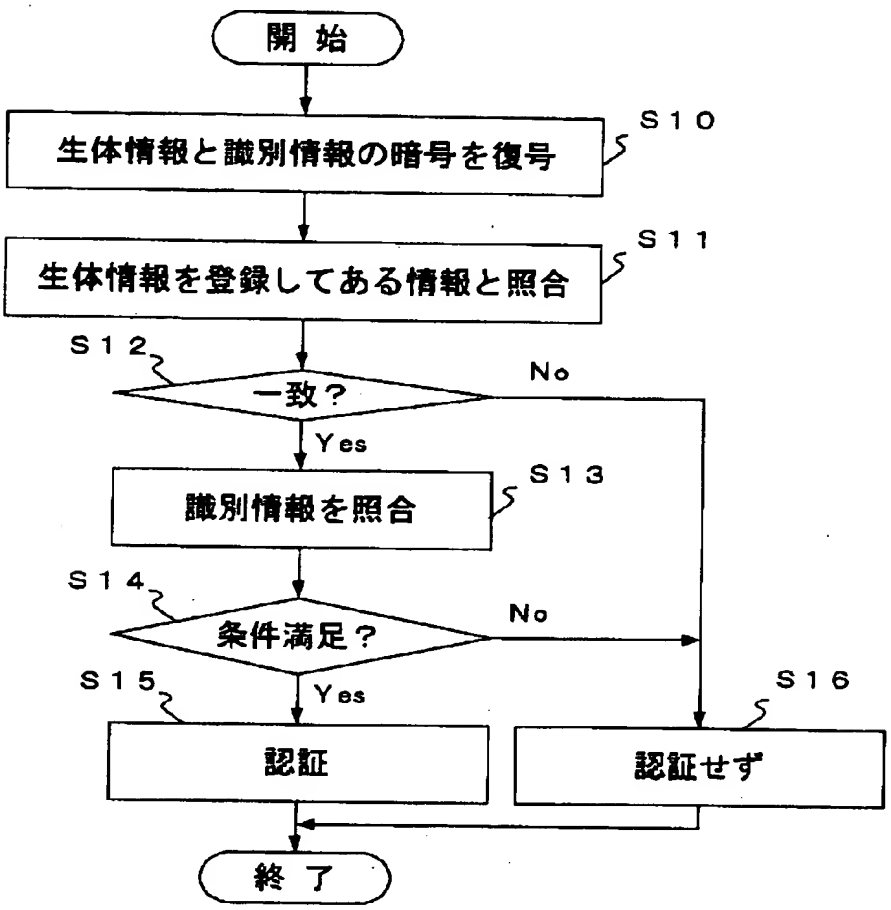
【図３】

第１の実施形態を実現する装置構成を示した図



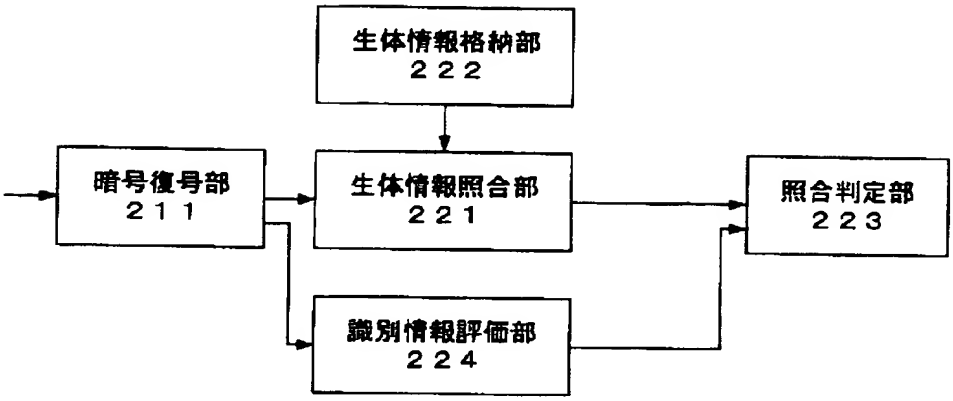
【図４】

図２の手順で生成した照合情報を用いて
本人認証を行う手順を示したフローチャート



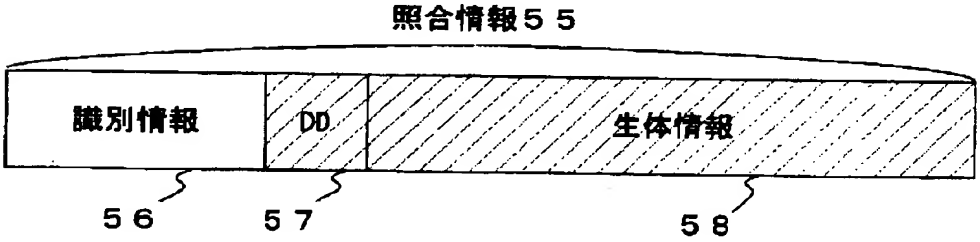
【図５】

図４の処理を行う装置の構成を示した図



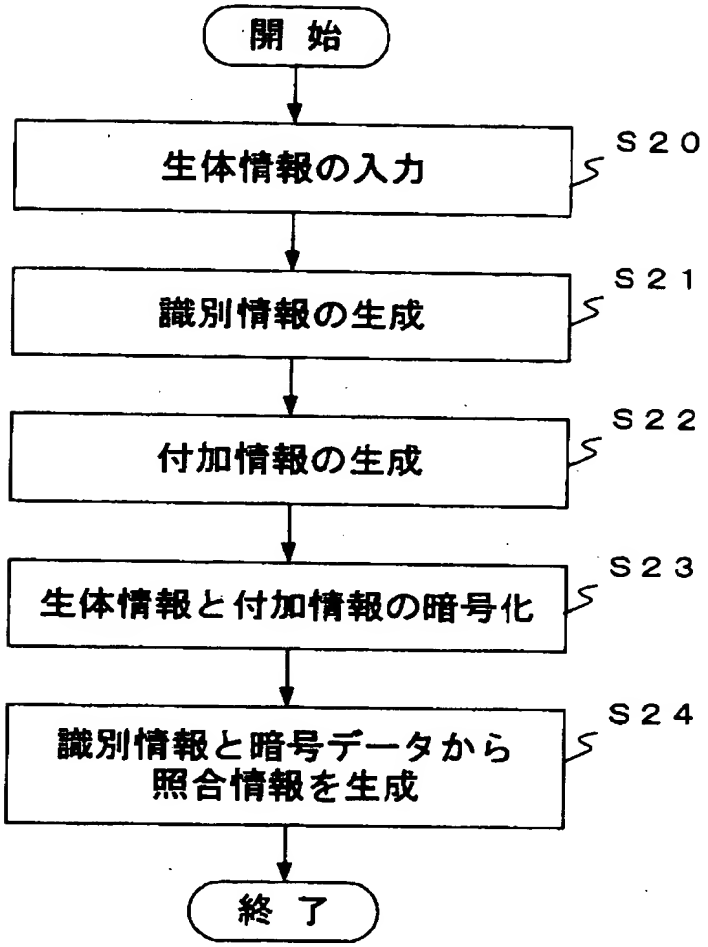
【図６】

本発明の第２の実施形態の照合情報の構成を示した図



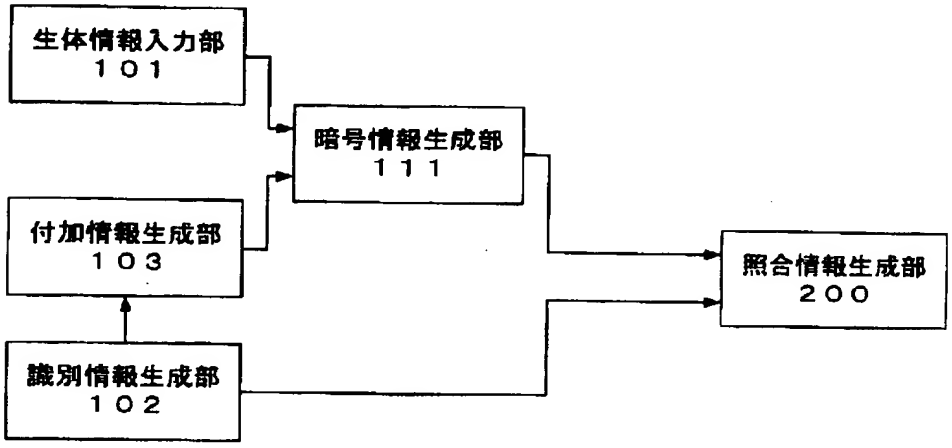
【図７】

本発明の第３の実施形態の
処理手順を示すフローチャート



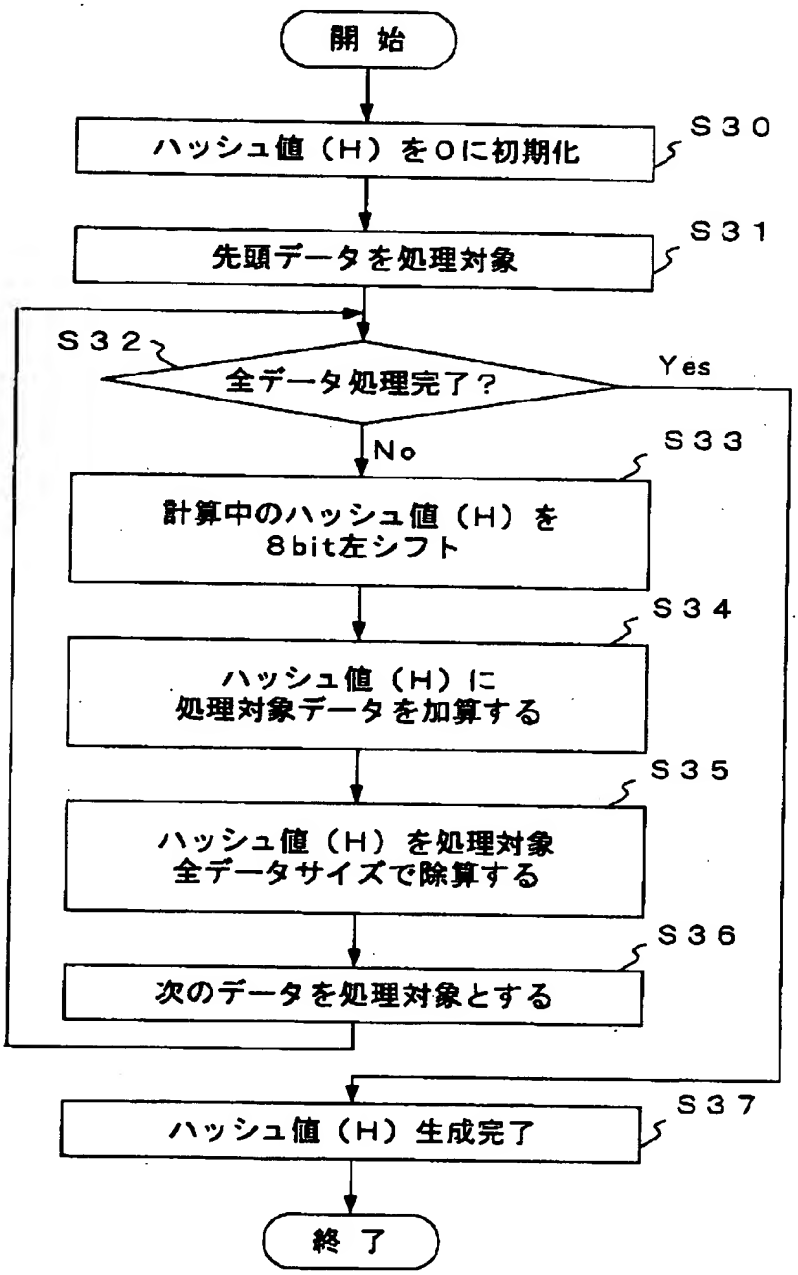
【図８】

第３の実施形態の照合情報生成のための装置構成を示す図



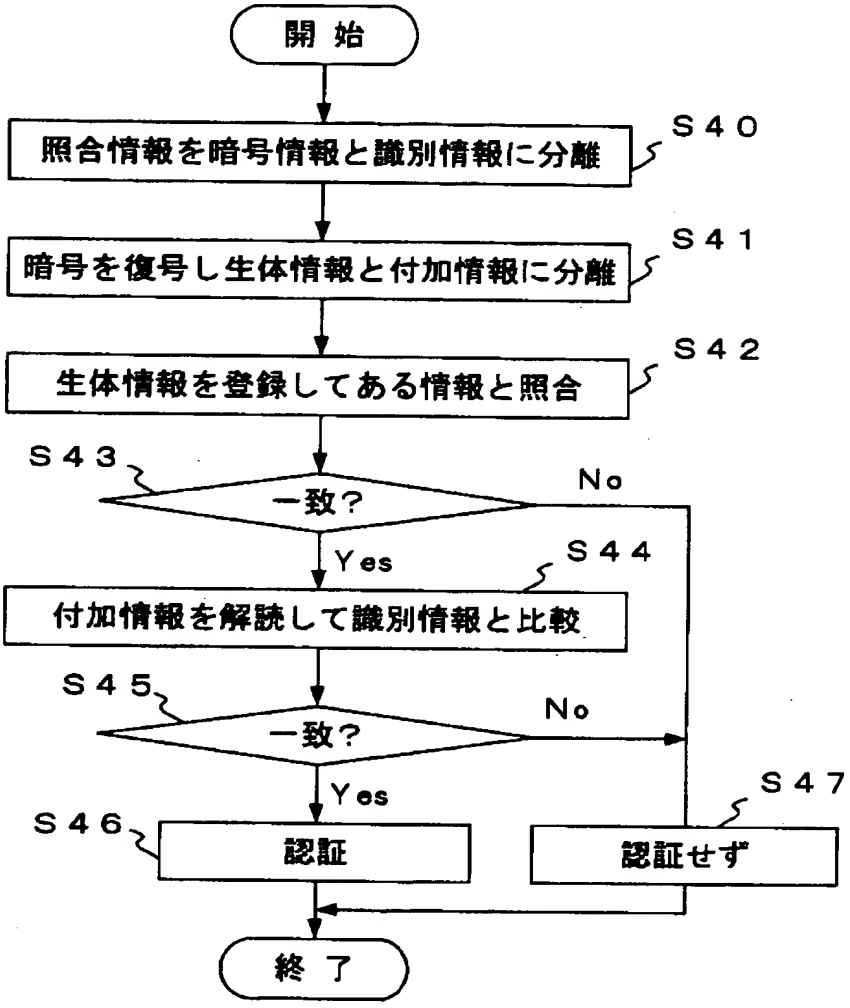
【図９】

付加情報の生成手順例を説明するフローチャート



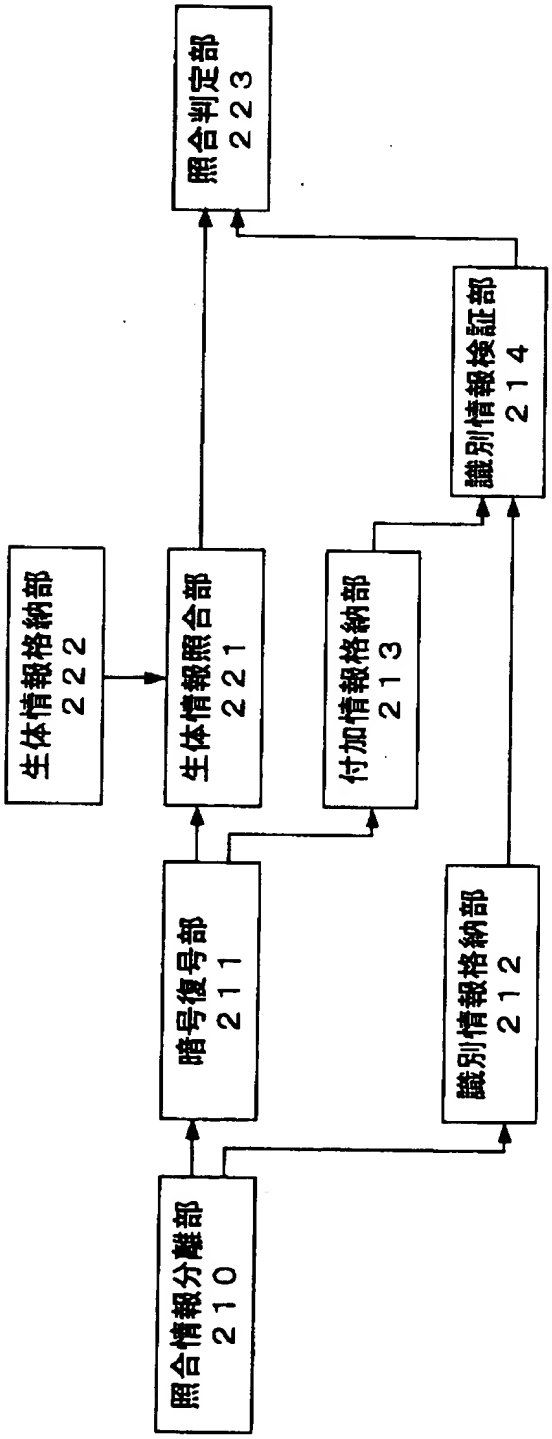
【図１０】

第３の実施形態において、
照合を実行する手順を示すフローチャート



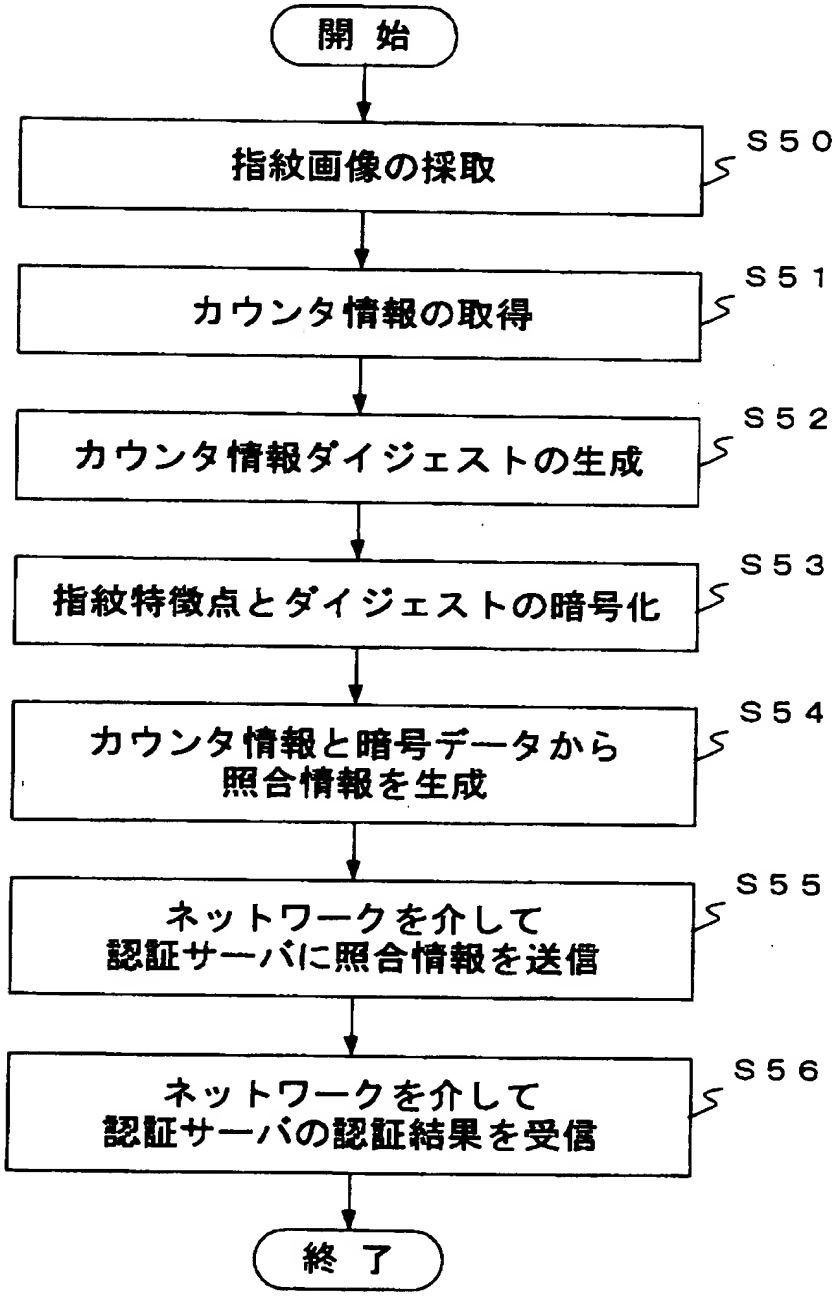
【図１１】

第３の実施形態における
照合部の構成を示した図



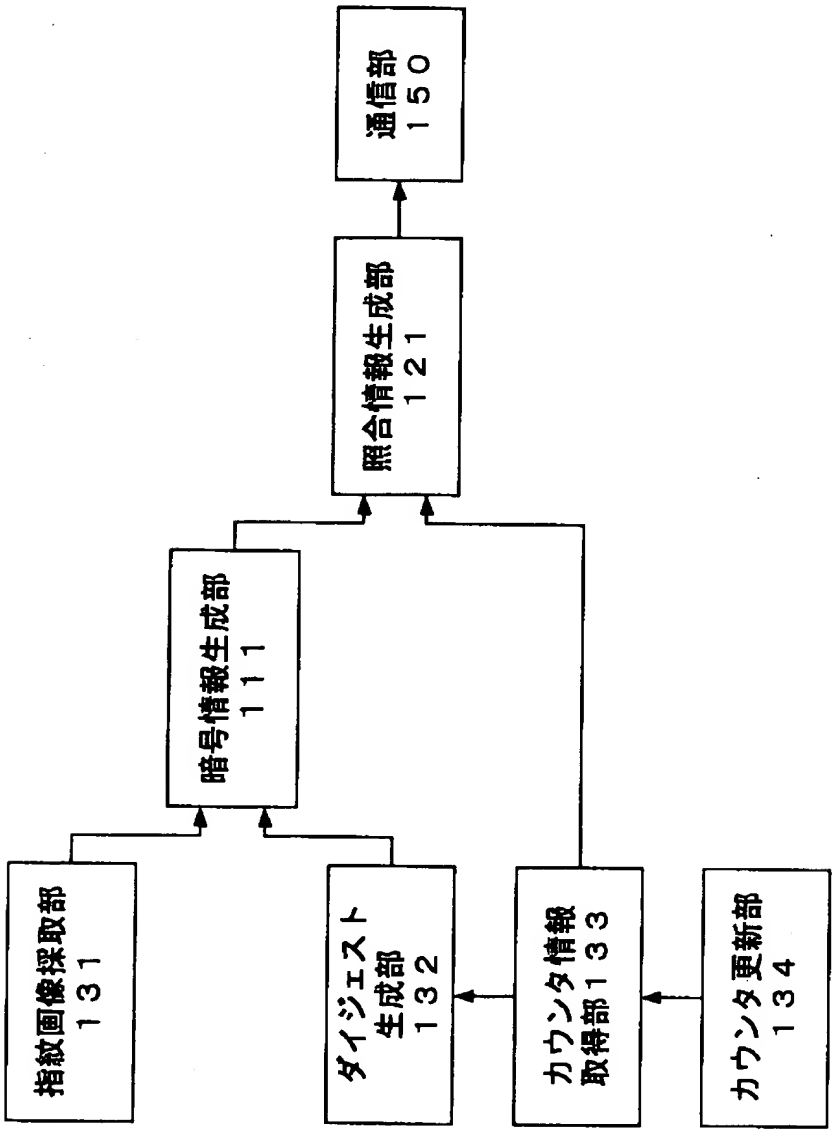
【図１２】

本発明の第４の実施形態の
照合情報生成手順を示すフローチャート



【図１３】

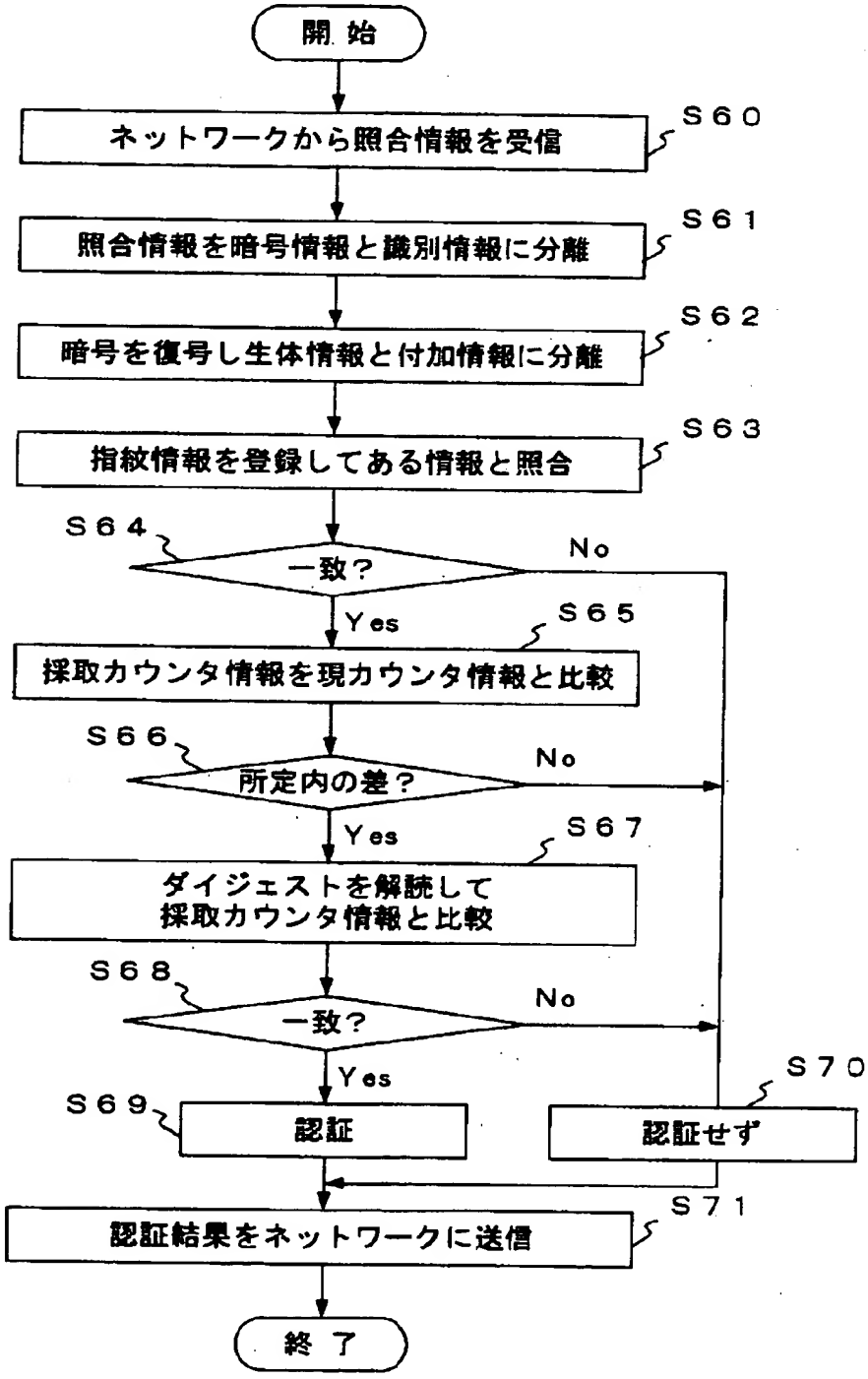
第4の実施形態の照合情報を生成する
端末装置の構成を説明する図



出証特２０００－３０４４６２６

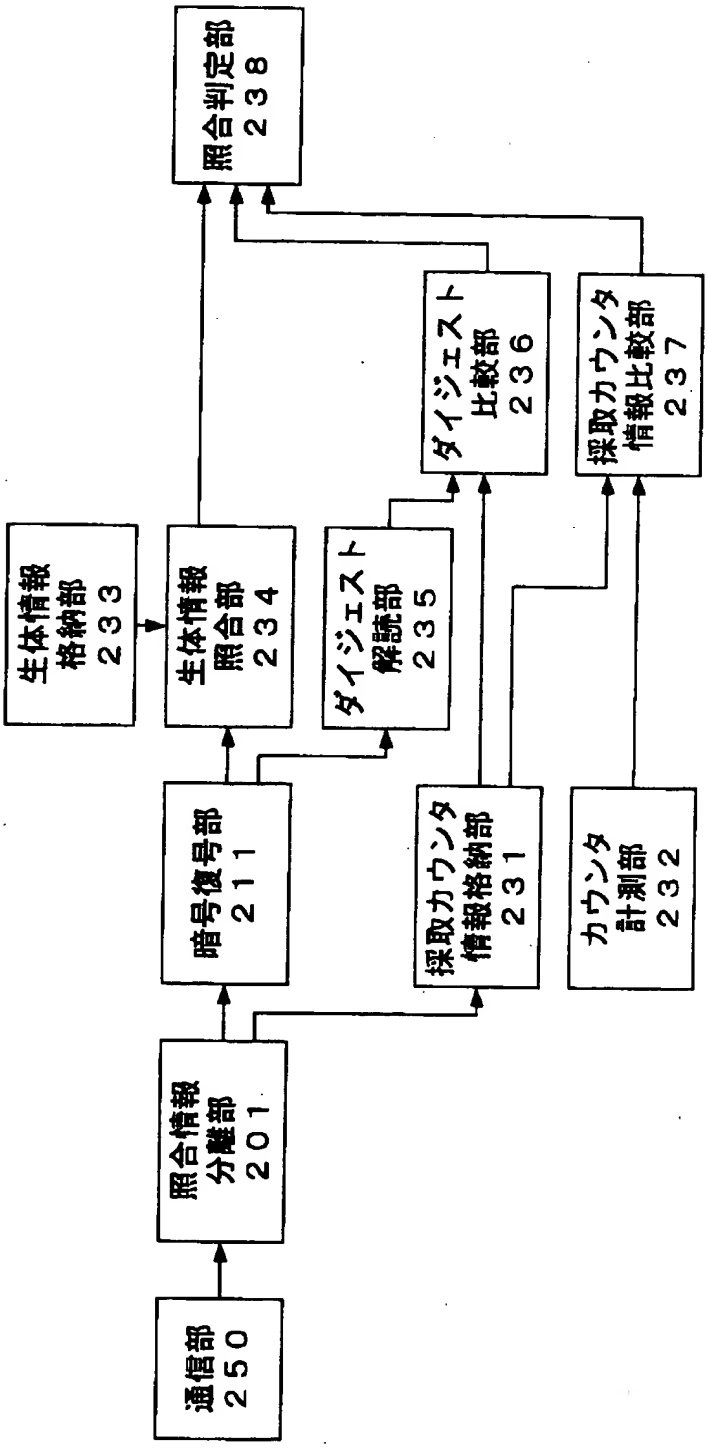
【図１４】

第４の実施形態の照合を行う
手順を説明するフローチャート



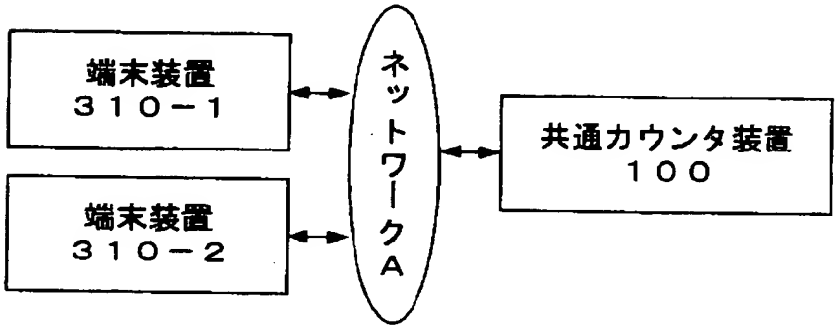
【図１５】

**第４の実施形態の
照合部の構成を説明する図**



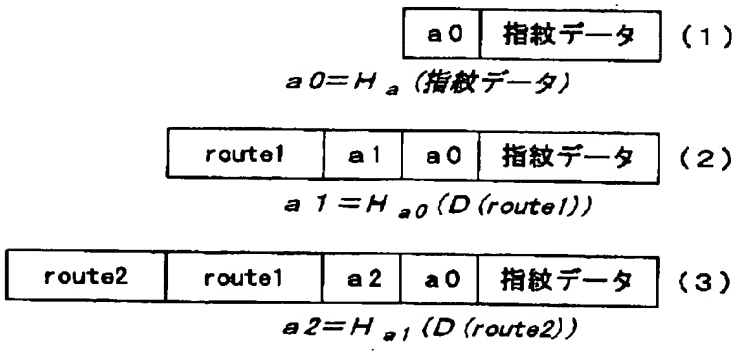
【図１６】

共通カウンタ情報を通信回線を経由して
端末装置が取得する実施形態の概略構成図



【図１７】

第５の実施形態のデータ構造を説明する図

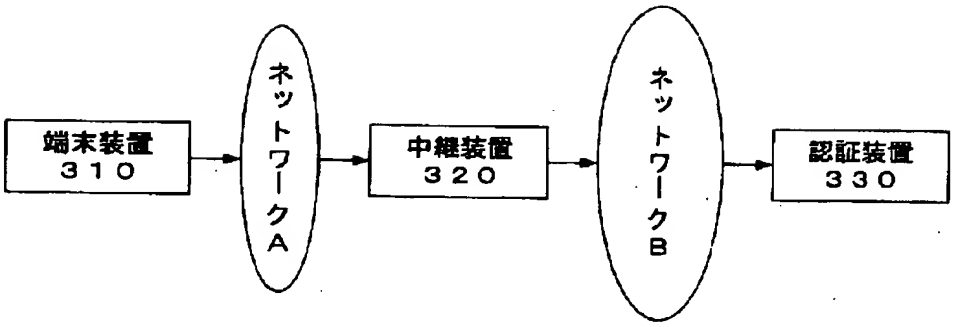


$H_a(x)$：パラメータaに関するxの一方向写像値（ハッシュ値）

D（x）：xのダイジェスト（ハッシュ値）

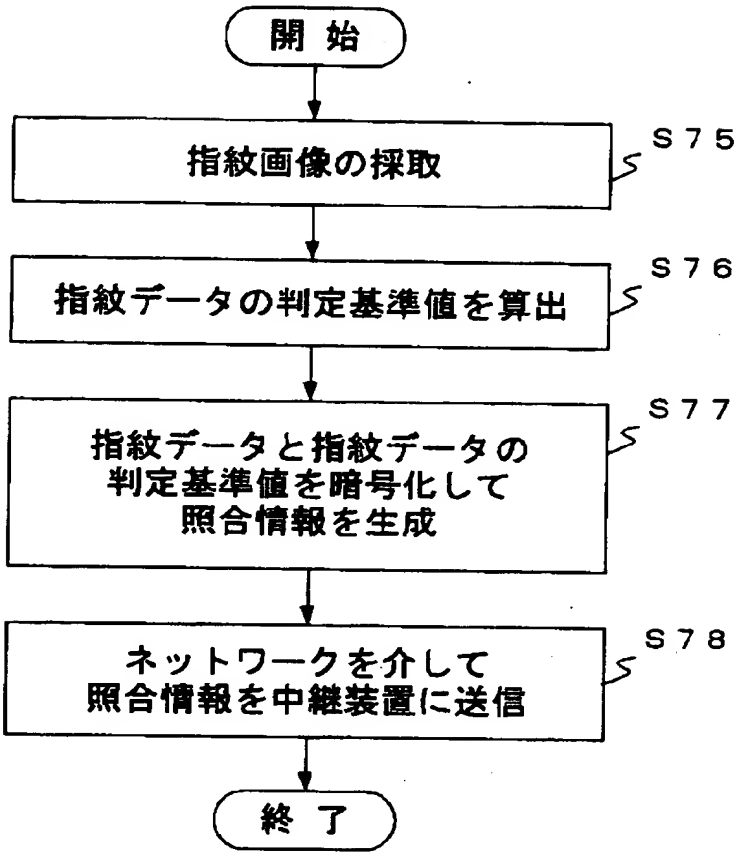
【図１８】

第５の実施形態のシステム構成を説明する図



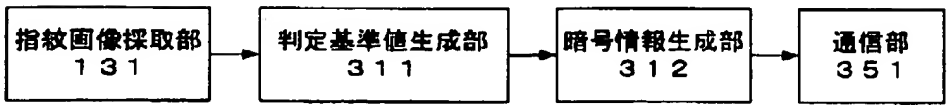
【図１９】

図１８の端末装置３１０が行う
処理手順を示すフローチャート



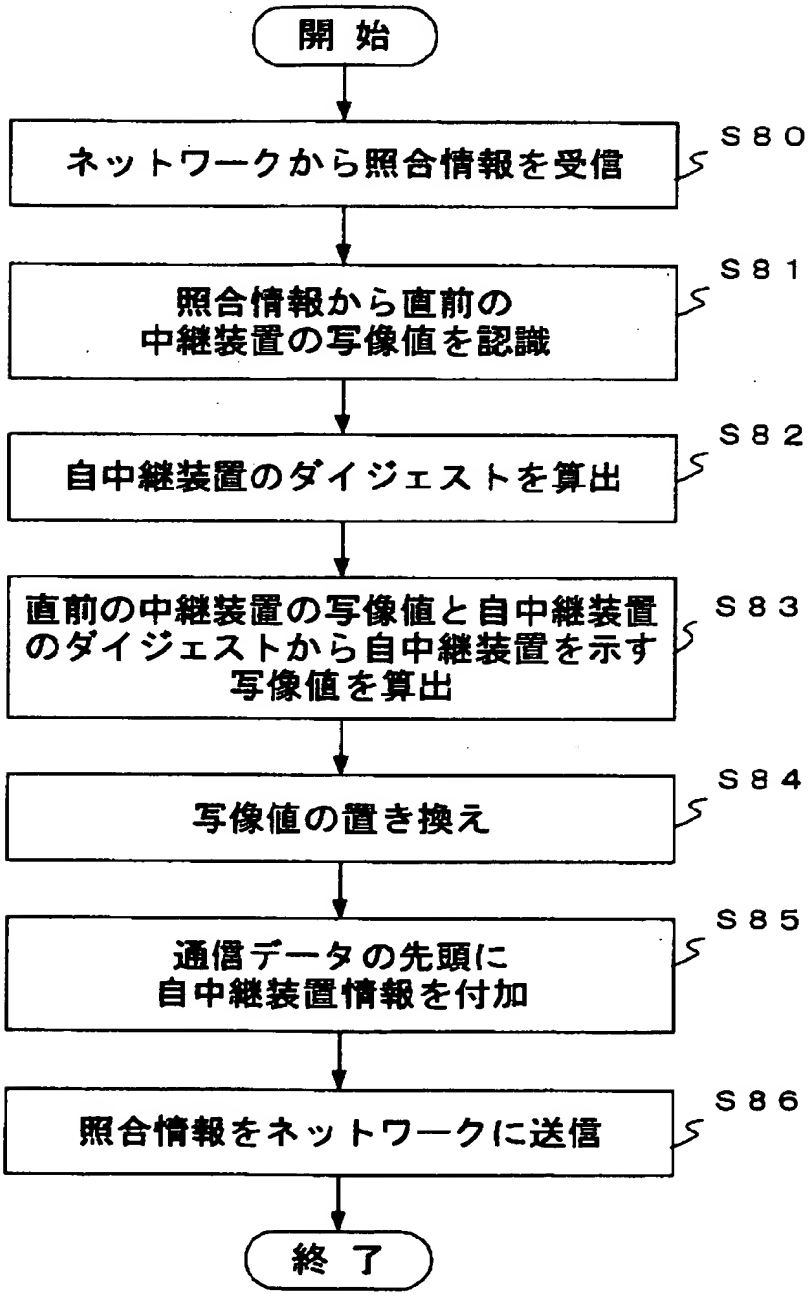
【図２０】

端末装置３１０の装置構成を説明する図



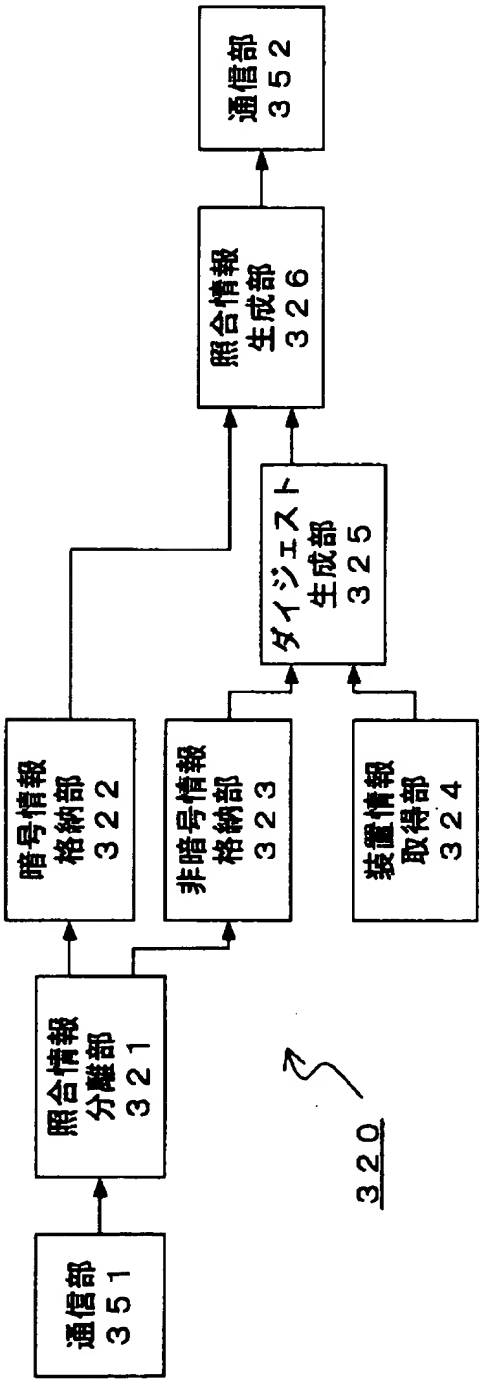
【図２１】

中継装置３２０の
処理手順を説明するフローチャート



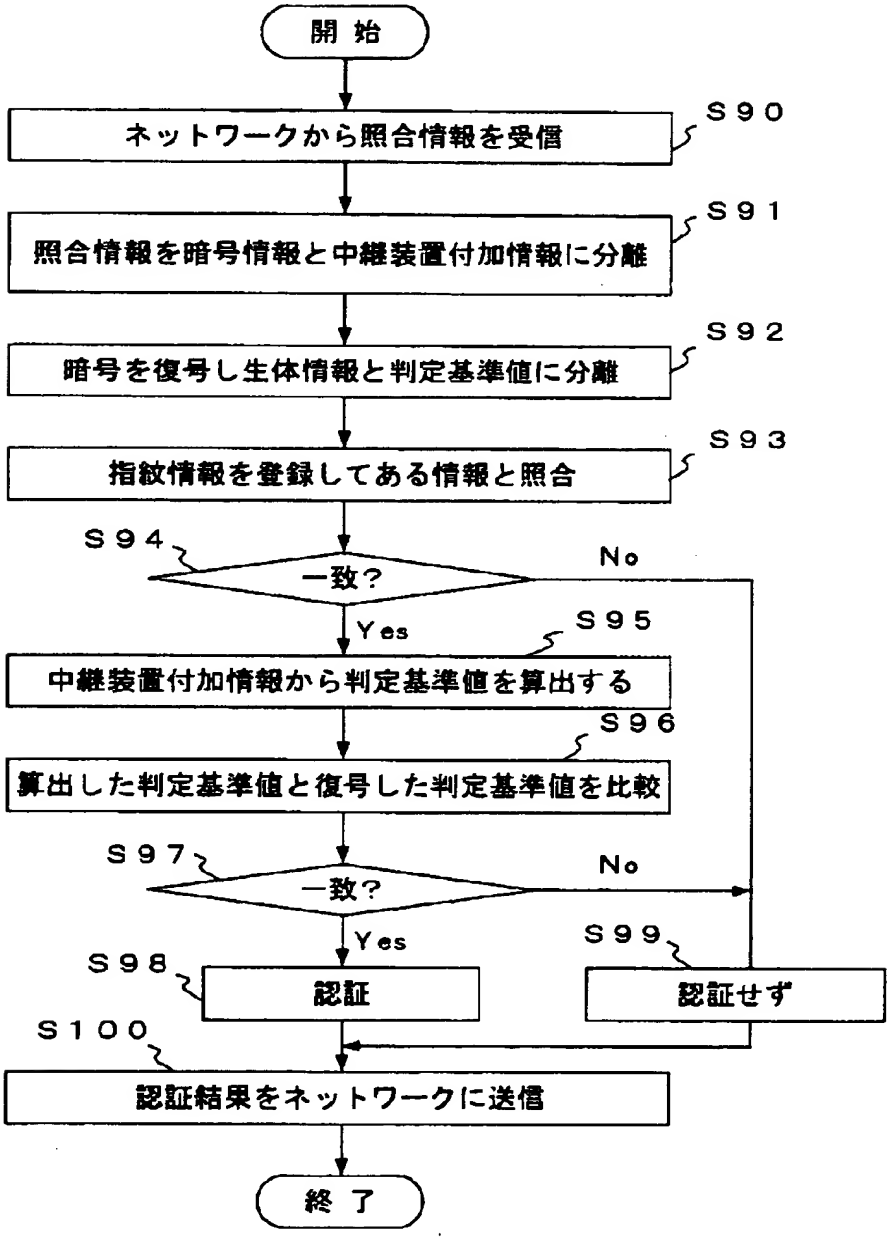
【図２２】

中継装置320の
装置構成を説明する図



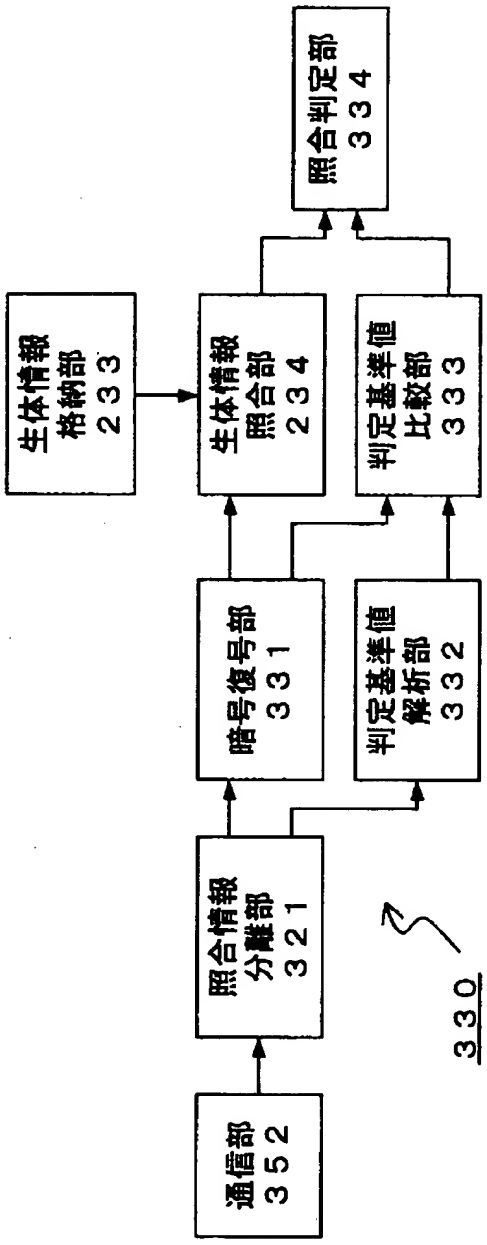
【図２３】

第５の実施形態における認証装置３３０の
動作手順を説明するフローチャート



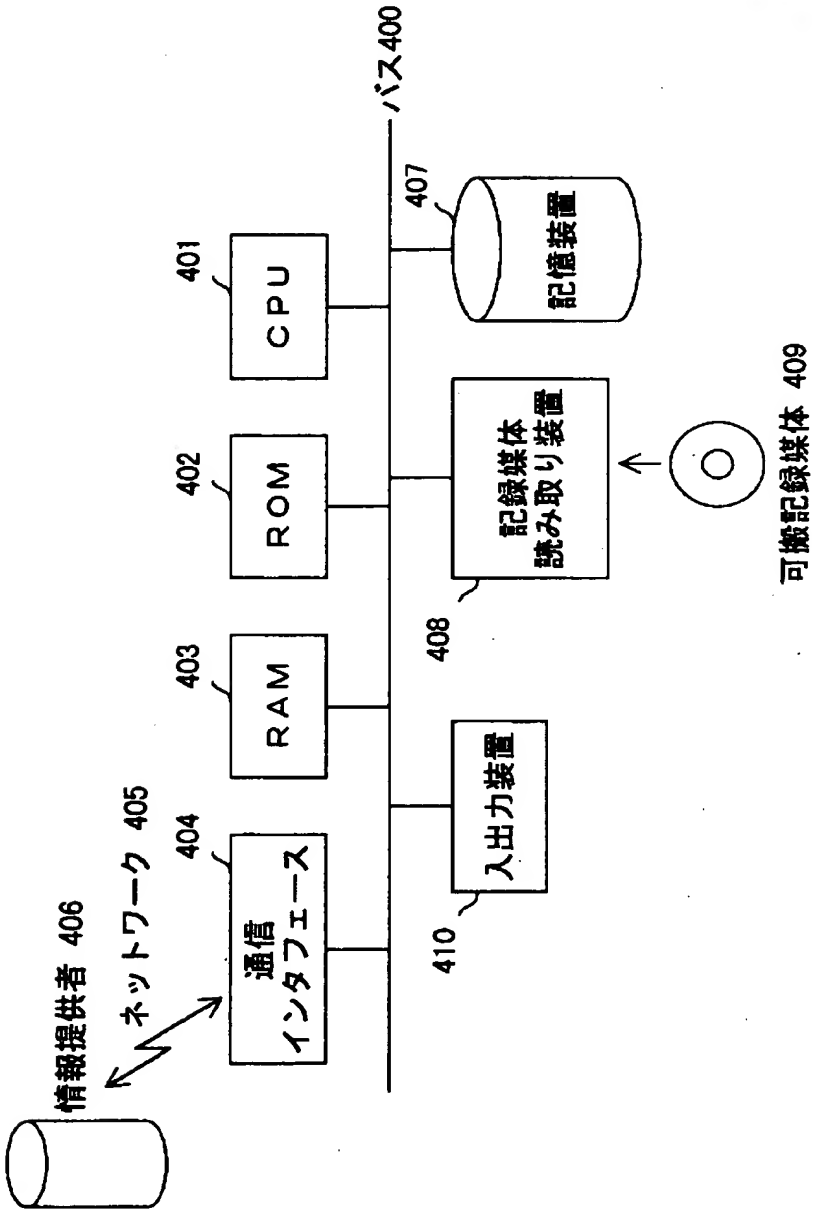
【図２４】

第５の実施形態の認証装置330
の装置構成を説明する図



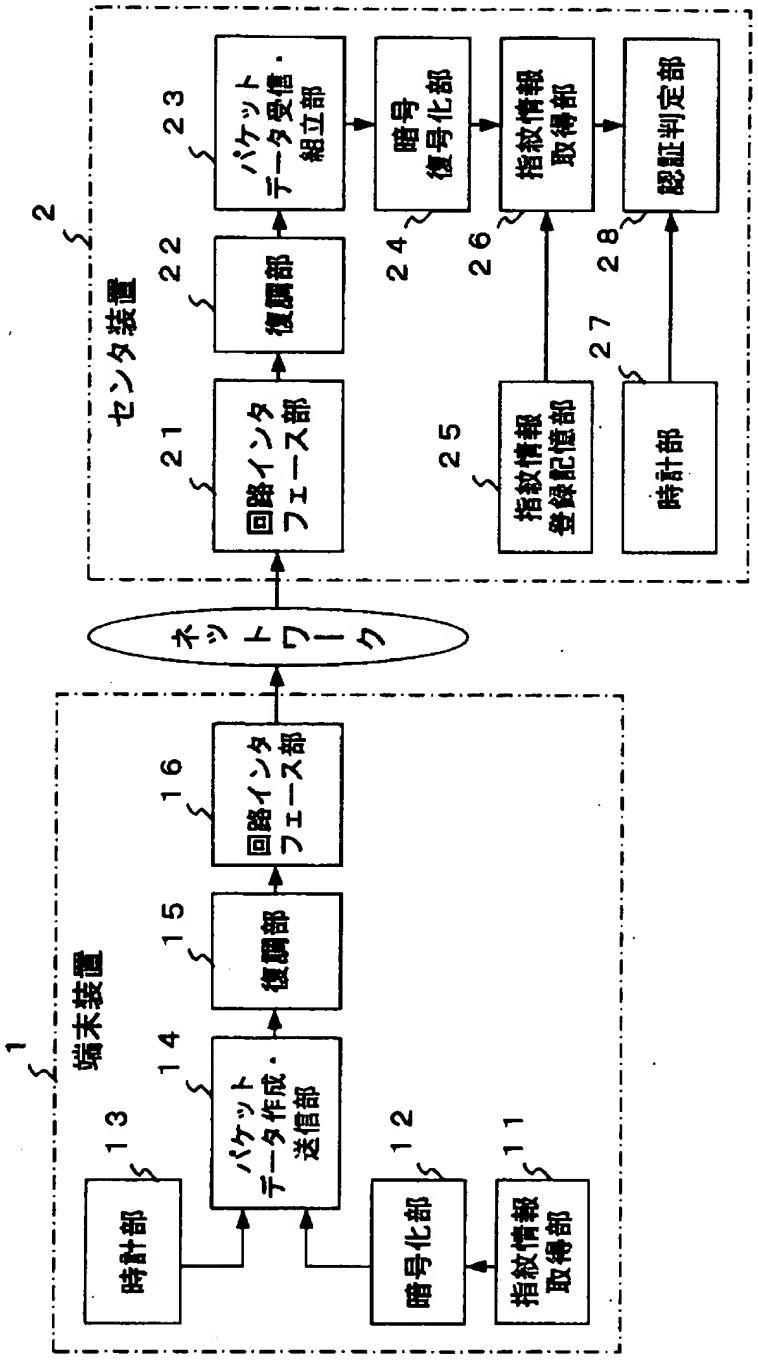
【図２５】

本発明の実施携帯をプログラムで実現する際に
必要とされるハードウェア環境を示す図



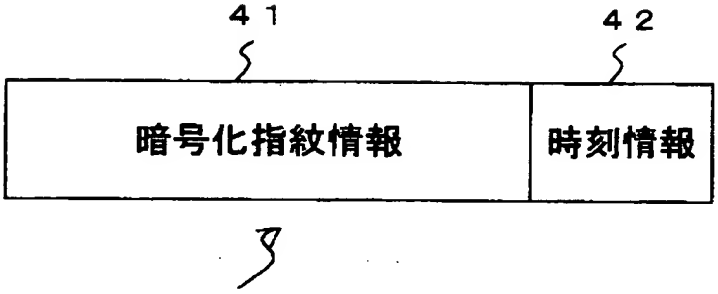
【図２６】

従来の生体情報を利用した
個人認証システムの構成例を示す図



【図２７】

従来のパケットデータの構成を示す図



【書類名】　　要約書

【要約】

【課題】生体情報を用いた個人認証システムにおいて、他人の「なりすまし」などを正確に排除することのできる生体情報を用いた認証装置及び方法を提供する。

【解決手段】照合情報５０は、指紋の特徴点情報などの生体情報と識別情報が組み合わされている。そして、識別情報としては、従来時刻情報を用いていたものを、生体情報を採取した装置のシリアル番号や装置名称、採取装置から認証を行う装置までの経路情報、あるいは、特定装置で採取した生体情報につけた一連番号などとする。そして、全体の照合情報５０を暗号化して、生体情報採取装置から照合装置にネットワークを介して送信する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社